TURING 图灵电子与电气工程丛书

WILEY

来自Nokia研究中心的3G技术名著

3G技术与UMTS网络

（第2版）

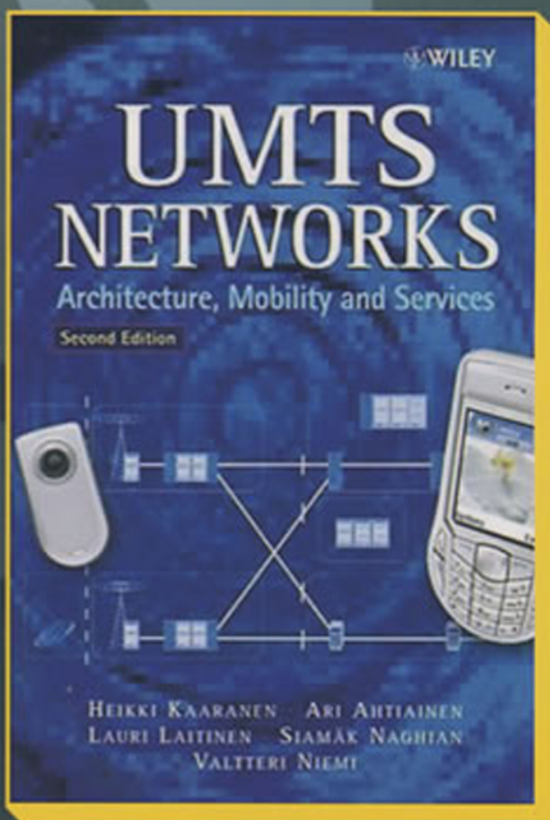
UMTS Networks

Architecture, Mobility and Services

(Second Edition)

Heikki Kaaranen
Ari Ahtiainen
[芬] Lauri Laitinen 著
Siamäk Naghian
Valtteri Niemi

彭木根 李安平 王文博 译
杨鸿文 审





人民邮电出版社
POSTS & TELECOM PRESS

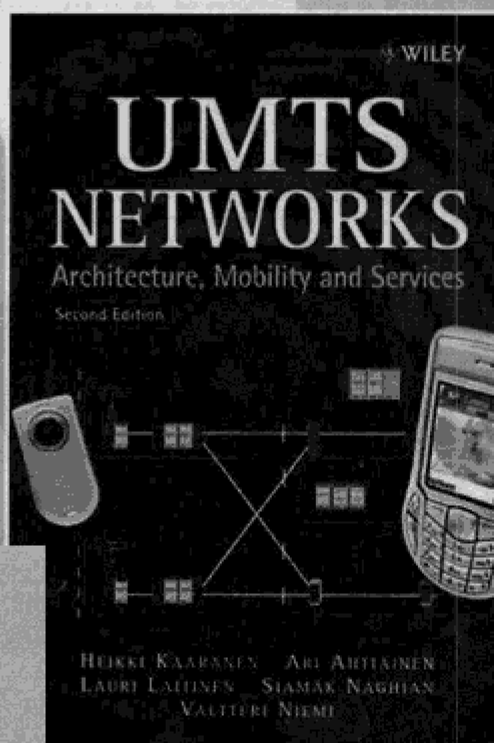
TURING 图灵电子与电气工程丛书

3G技术与UMTS网络（第2版）

UMTS Networks
Architecture, Mobility and Services
(Second Edition)

[芬] Heikki Kaaranen
Ari Ahtiainen
Lauri Laitinen
Siamäk Naghian
Valtteri Niemi 著

彭木根 李安平 王文博 译
杨鸿文 审



人民邮电出版社
北京

图书在版编目（C I P）数据

3G技术与UMTS网络：第2版 / （芬）卡拉宁（Kaaranen, H.）等著；彭木根，李安平，王文博译. —北京：人民邮电出版社，2008. 12
（图灵电子与电气工程丛书）
书名原文:UMTS Networks：Architecture，Mobility and Services
ISBN 978-7-115-18772-7

I. 3… II. ①卡…②彭…③李…④王… III. 移动通信—通信系统 IV. TN929. 5

中国版本图书馆CIP数据核字（2008）第136014号

内 容 提 要

本书是一本全面介绍3G系统特别是通用移动通信系统(UMTS)网络的专著。本书的一大特色是详细介绍了WCDMA标准所采用的UMTS网络,包括UMTS的网络演化、网络结构和组成、移动管理和业务等。本书深入阐述了移动通信的发展和演化、UMTS的系统设计、UMTS网络架构和协议组成、UMTS的空中接口技术原理、UMTS核心网技术和UMTS网络协议等。

本书内容翔实,针对性强,适合于移动通信领域的管理和科研人员阅读参考,也可作为大专院校相关专业的教材。

图灵电子与电气工程丛书
3G 技术与 UMTS 网络

◆ 著　［芬］Heikki Kaaranen Ari Ahtiainen Lauri Laitinen Siamäk Naghian Valtteri Niemi
译　彭木根　李安平　王文博
审　杨鸿文
责任编辑　舒　立

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
邮编 100061　电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：21.5
字数：445千字　2008年12月第1版
印数：1－4 000册　2008年12月北京第1次印刷

著作权合同登记号　图字：01-2006-3164号
ISBN 978-7-115-18772-7/TN

定价：59.00元

读者服务热线：(010)88593802　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　　言

1991年7月1日，在芬兰赫尔辛基的一个城市公园中进行了世界上第一次基于公共GSM系统的通话，这是第二代移动通信系统诞生的标志。GSM系统取得了出乎预料的巨大成功。在过去的十年中，GSM已经成为真正意义上的全球移动通信系统。目前，蜂窝移动电话在很多国家的持有率已经超过了70%，在北欧国家已经接近了90%，而且，全球移动用户的数量已经超过了固定电话用户的数量。在不久的将来，移动用户的数量将会超过预计的15亿。

在十多年后的今天，随着GSM系统的不断发展，它开始向第三代移动通信系统——UMTS（通用移动通信系统，Universal Mobile Telecommunications System）演进。基于UMTS的第一个网络已经开始运行，而设想的新一代移动电话已经出现。到2004年10月底，全世界共有50个用于商业的UMTS商务网络开始运营。

为了获得更广的应用，UMTS网络引入了一种全新的高速无线技术，即WCDMA（宽带码分多址，Wideband Code Division Multiple Access）。然而，UMTS系统的核心网部分将建立在成功的GSM网络基础之上。GSM网络已经从电路交换的语音网络向移动分组数据业务（如短消息、移动网页浏览和移动Email接入）的全球平台演进。

最新的预测表明，在不久的将来移动核心网提供的分组交换业务将超过电路交换业务。这种转变是因使用UMTS系统而实现的。通过使用UMTS系统，网络运营商才可以提供同样可靠的电路交换和分组交换平台来满足数据速率和容量的需求。大多数的语音和对时间敏感的数据业务仍然需要采用电路交换技术，而对时间不敏感的数据则可以通过UMTS系统的分组数据核心网传输。

UMTS移动计算和通信设备的一个主要优点，在于它能够随时随地向用户传递信息。在UMTS系统中，移动电话成为人们信赖的设备，一种工作和休闲的生活工具。在未来可能的通信业务中，娱乐和商务应用将是通话和多媒体数据业务的新类型，用户及其终端的移动性和个性化将会促进这些业务的不断发展。

本书主要介绍UMTS网络如何作为移动性和各种业务支持的第三代平台，旨在全面综述系统结构及其演化过程，可以作为读者学习3GPP协议的指南。本书可以分为三个部分。

第一部分由第1章和第2章组成，对UMTS系统做了总体的概述。第1章主要介绍UMTS技术、业务结构和关键的系统概念。第2章介绍了移动网络从第二代GSM到第一个UMTS多接入版本的演化过程，同时介绍了此后UMTS系统如何向全IP移

动网络演化。

第二部分由第3章至第9章组成,详细介绍无线技术、无线接入和核心网等方面的内容,并详细讲述关于终端方面的内容,解释了提供给终端用户的功能和业务。第3章主要概述了蜂窝网络(尤其是在UMTS系统)所面临的关键的结构设计上的一些挑战,并给出解决这些问题的方法。

第4章主要对UMTS接入技术进行了概述,包括在3GPP R5范围内WCDMA技术中的最新增强。除此之外,还讲述了一些其他的接入技术,如GSM/EDGE与WLAN,这些都是对UMTS多接入网络的补充。

第5章和第6章描述了分布于无线接入UMTS网络单元中各控制功能和核心网之间的功能划分。第7章对UMTS用户设备做了概述,主要讲述UMTS网络以外的其他可见部分。第8章讨论了UMTS网络的业务。通过对QoS(服务质量)的描述及给出一些由UMTS带来的业务例子来讲述业务的实现问题。UMTS网络的先进安全解决方案在第9章中讨论。

第10章和第11章构成了本书的第三部分。这部分主要从协议的角度描述了不同结构单元之间系统范围内的互操作(interworking)。第10章首先详细介绍了基本的UMTS协议结构,然后对系统的各协议逐一进行了介绍。第11章回到前几章网络的角度,通过给出几个精选的系统过程实例,探讨了如何在系统协议的协调下,跨UMTS网络接口完成业务传输的功能。

第三代移动通信系统正在方兴未艾,成千上万的主流系统和软件工程师、内容提供商、应用开发商、系统集成商和网络运营商的支持将进一步促使UMTS系统获得成功。我们希望本书能帮助所有的同仁实现自己的目标,能使大家享受UMTS网络环境并从中获益。

本书的所有内容只代表作者本人的看法和观点,不一定代表其使用者的看法。

第 2 版新增内容

自从 2001 年本书的第 1 版出版以来，无线通信技术出现了许多新的变化，尤其在 UTMS 网络发展方面。以数据为中心的业务成为潮流，UMTS 网络在一些国家已经实现，移动电话已经能够集成包括 WLAN（无线局域网）和蓝牙在内的短距离无线通信，因特网的使用迅速发展，移动网与 IP 网的融合更为明显。在 3GPP R5 的最新进展中，这些都以这样或那样的方式实现。这个新版本将尽量反映这些新的变化，同时继续定位于全面描述 UMTS 的系统结构。对于本书的第 1 版，我们还收到了来自世界各地读者的很多宝贵意见。我们对这些深入的见解深表感谢，第 2 版的编写过程中已经考虑了这些意见。反馈意见使我们更有信心，本书作为一本 UMTS 系统结构方面的参考书的初衷已被读者接受。第 1 版也被许多培训部门、研究机构和大学用作教材。在考虑读者意见时，我们也充分考虑了这一因素。此外，新版在提高整体质量方面作出了更多的努力。为此，无论是作者还是出版商，都对本书的编辑和校对工作付出了更多的精力。

新版对每章都进行了修订，以反映 3GPP 标准到 R5 的发展。部分章节进行了较大的结构调整和改进。新版的主要修改如下。

- 第 1 版中 UMTS 网络看作单一的接入网络，只能通过 WCDMA UTRAN 接入网识别，所有论述都以此为基础。该新版考虑了其他一些接入技术。新版对 UTRAN 的处理和先前一样。鉴于 GSM 形成了基本覆盖，故此突出了基本的 GSM 技术。鉴于补充接入技术的互通已成为 3GPP 演进的一个组成部分，故对此做了简要介绍。
- 第 1 章和第 2 章做了一些小的改动，一些图做了修改，以适应 3GPP R5。
- 鉴于不同的接入技术，旧版中的第 3 章现在分成了两章（第 3 章与第 4 章）。新版的第 3 章回顾了由无线通信的限制、设备移动性、传输、网管和频谱稀缺性等带来的对无线网络的挑战。第 4 章对所选的 UMTS 接入技术进行了概述，包括 WCDMA 及其加强版 HSPDA、GSM/EDGE 和 WLAN。
- 对第 5 章 UTRNA 进行了修订和细调，增加了 HSPDA。对第 6 章核心网进行较大的修订，并描述了 IMS 结构和功能。这些补充反映了 R5 中的一些主要内容。
- 第 7 章终端没有大的改动，只是增加了与 IMS 相关的内容。第 8 章业务则是整章重写的。

- 第9章、第10章、第11章都已更新到3GPP R5。

这些修改使全书比旧版增加了大约100页，使新版能完全兼容3GPP R5标准。

此外可向Heikki Kaaranen索取本书PDF格式的幻灯片，进一步的信息和详细的订购咨询请发送邮件到heikki.kaaranen@aquarecords.fi或登录网站www.aquarecords.fi。

致 谢

在写作本书第1版的过程中，作者和参与人员有幸赶上了UMTS系统标准最终定案的激动时刻。在写第2版的时候，我们又见证了另一个激动人心的时刻：UMTS网络在世界范围内得到应用。来自Nokia公司内外的许多同行对本书的各个方面提供了宝贵的资料和意见。我们特别感谢Seppo Alanara、Mika Forssell、Harri Holma、Kaisu Iisakkila、Tatjana Issayeva、Sarni Kekki、Pekka Korja、Jan Kåll、Juho Laatu、John Loughney、Atte Länsisalmi、Anna Markkanen、Tomi Mikkonen、Juha Mikola、Ahti Muhonen、Aki Niemi、Mikko Puuskari、Mikko J. Rinne、Ville Ruutu、Juha Sipilä、Janne Tervonen、Mikko Tirronen、Ari Tourunen、Jukka Vialén和Andrei Zimenkov。

令人鼓舞的工作环境，以及与Nokia公司研发和标准化项目团队的密切联系离不开下列项目经理：Kari Aaltonen、Heikki Ahava、Tapio Harila、Reijo Juvonen、Jari Lehmusvuori、Juhani Kuusi、Yrjö Neuvo、Tero Ojanperä、Lauri Oksanen、Pertti Paski、Tuula-Mari Rautala、Tuomo Sipilä、Jukka Soikkeli、Jari Vainikka和Asko Vilavaara。由Mark Hammond和Sarah Hinton带领的John Wiley & Sons出版团队对本书第2版成书提供了有力的支持。他们努力工作的精神使得本书能在规定的时间内顺利完成。Bruce Shuttlewood以及Originator Publishing Services对英文版原书进行了编辑，解决了语句问题，增强了可读性。

我们不应忘记这是一本关于UMTS网络的书，这些网络是无数同行协作设计和研究的成果，正是这些专家的宝贵意见才使UMTS问世。这里不能一一列出20世纪90年代初以来3GPP组织和参与UMTS发展的所有专家，感谢他们为开创移动通信的新纪元所做的贡献。

最后要感谢我们的家人，感谢他们在本书的长期撰写和夜以继日的工作期间给予的耐心支持。特别要感谢Satu Kangasjärvelä-Kaaranen夫人，在将初稿汇总时，她所做的文字处理和一些图的设计是非常重要的。

我们有义务不断改进本书，再次欢迎任何的意见和建议，以便将来在下一版中修改。请发电子邮件到umtsnetworks@pcuf.fi。

作者

赫尔辛基，芬兰

目　　录

第三部分

第一部分



第 1 章
绪论

今天,三代不同的、已经实现了的移动通信已广为人知(如图 1.1 所示)。第一代(1G)是 20 世纪 80 年代中期建立的模拟或半模拟(模拟无线信道,但是采用数字交换)移动网络,例如 NMT(北欧移动电话)系统和 AMPS(美国移动电话系统)。这些网络为用户提供基本业务,主要是话音及和话音相关的业务。1G 网络仅仅是以一国为范围而开发的,经常出现的情形是政府的电信运营商和国内行业就主要技术要求达成一致,并不在更大范围内发行标准。由于是国家性的标准,不同的 1G 网络彼此互不兼容,而且在当时,移动通信被认为是一种新奇的事物,是固网上的增值业务。



图 1.1　各代蜂窝系统

移动通信需求的增长产生了对更为全球化的移动通信系统的需求。国际性的标准化组织开始具体指定 2G(第二代)应该是什么样子。2G 的重点着眼于兼容性和国际透明度,系统应当是区域性的(例如欧洲范围)或是半全球性的,用户基本上应该能

在这个范围内的任何地点接入系统。从终端用户的角度看,2G 网络是一个更具吸引力的“套餐”,除了传统的语音业务外,它还能提供一些数据业务和高级的补充业务。标准化的区域特性使全球化这个概念没有完全实现,市场上并存着多种 2G 系统。其中 GSM(全球移动通信系统)以其改进系统成为商业成功的神话,无论是技术方面还是商业方面,它都超越了人们的种种预想。

人们期望 3G(第三代)能够完成移动通信的全球化进程。但不同国家和区域的利益冲突仍然存在,其难度也是可想而知的。不过大势所趋的是,3G 将主要基于 GSM 的技术解决方案,其原因有以下两点:GSM 技术主导着市场,对 GSM 的巨大投资应当尽可能地利用。鉴于此,标准化组织提出了未来 10 年中移动通信将如何发展的愿景。在这个愿景中,对 3G 的一些要求简列如下。

(1)系统必须完全规范化(如 GSM),主要接口应当是标准化的和开放的。所形成的标准必须在全球范围内有效。

(2)系统相对于 GSM 在各个方面都要有明显的增值。但在初期,系统至少应后向兼容 GSM 和 ISDN(综合业务数字网)。

(3)在整个系统中,多媒体及其所有的组成部分都必须获得支持。

(4)3G 的无线接入必须能提供宽带容量,这个容量应具有足够的一般性以适用于全世界。宽带(wideband)这个词反映了它的容量要求介于 2G 的窄带容量和固定通信介质的广带(broadband)容量之间。

(5)终端用户的业务应独立于无线接入技术的细节,网络架构不得限制这些业务的产生。也就是说,技术平台是一回事,使用平台的业务又完全是另一回事。

在 3G 标准化工作进行的同时,主要的电信发展趋势也在改变。传统的电信领域和迄今为止分离的数据通信(即因特网)开始快速融合。这已经形成了一个发展链,其中传统电信和 IP 技术将融合在同一包内。这个大趋势有多种说法,据个人观点而定。一些人称这种发展的目标是“移动信息社会”或者“移动 IP”,另一些人称其为“3G ALL IP”,其些商业背景中还有“E2E IP”(End-to-End IP)的说法。按 3G 的定义看,全面的 IP 实现是 3G 发展的必由之路。

3G 系统已进入一个新的阶段,旨在建立 4G 规范的工作实际上也已经拉开了帷幕。现在来预测 3G 演进将在何时结束,4G 将在何时真正开始还为时尚早。未来的发展更应当看成是一个不断发展的链条,3G 将会继续提出新的方法来处理和融合各种类型的数据和移动性。然后,4G 将带给终端用户更大的容量和更多的增值,以更成熟的系统概念出现。

1.1 3G 的标准化进程

欧洲国家 GSM 标准的统一性造就了移动通信全球化的可能性。当我们看到日本的 2G PDC(太平洋数字通信系统)未能扩展到远东而开放的 GSM 标准被大多数亚洲

市场所采用，当我们看到GSM的变型也成为美国PCS(个人通信系统)市场可选的国家标准之一时，这种可能性就变得更为明显。

一个公共的全球移动通信系统自然会产生许多政治意图。在3G的例子中，单从系统的命名方式就能看出这一点。最中立的名字是“第三代”，即3G。世界的不同地方强调的因素不同，使全球性的3G这个词有了许多地区性的同义词。3G在欧洲成了UMTS(通用移动通信系统)，这是ETSI(欧洲电信标准化协会)的观点。在日本和美国，3G的名字经常是IMT-2000(国际移动电话2000)，来自于ITU(国际电信联盟)发展计划。美国的CDMA2000(码分多址)也是3G蜂窝系统，代表从IS-95系统的演进。本书将要介绍的是UMTS系统，它已经被世界性的3GPP(3G合作者计划)标准化。为了规范某种程度上让人感到混乱的命名方式，3GPP决定，3G的正式名称是“3GPP系统”，后面必须带一个反映整体规范的版本号。因此，欧式UMTS网络的第一个版本的正式名称是“3GPP R99”。虽然有这个规定，上述UMTS和IMT-2000名称仍在广泛使用。

UMTS初期大量继承了GSM中的元素和功能规则，最可观的新发展在于网络的无线接入部分。UMTS引入了一个更先进的接入技术(即宽带式无线接入)。WCDMA(宽带码分多址)由CDMA演进而来，CDMA是一个经过了验证的技术，已经用于军事目的和窄带蜂窝网络，尤其在美国。

UMTS的标准化由欧盟创建并资助的几个预标准化研究项目所推进。1992年~1995年，RACE(欧洲先进通信研究)MoNet计划开发出建模技术，来描述无线接入和网络的核心部分之间的功能分配。例如，需要这种建模技术比较智能网和GSM MAP(移动应用部分)协议作为移动性管理的解决方案。除了讨论采用窄带还是宽带ISDN外，移动性管理方案是MoNet中的主要分歧之一。此外，MoNet计划末期还提起过采用ATM(异步传输模式)和B-ISDN作为固定传输技术的问题。

1995年~1998年，3G研究在ACTS(先进通信技术与服务)FRAMES(未来无线宽带多址接入系统)计划中继续进行。前几年的工作是选择和开发合适的多址接入技术，主要考虑的是CDMA和TDMA(时分多址)。欧洲大的制造商更倾向于TDMA，因为它也在GSM使用。基于CDMA的技术主要是美国行业在推广，他们对这种技术有经验，因为早先在国防设备上用过。

ITU期望至少规范一种通用的全球无线接口技术。这种协调工作是作为FPLMTS(未来公用陆地移动通信系统)进行的，后来更名为IMT-2000。许多区域性标准化组织的并行工作促成了IMT-2000系统家庭中的通用结构准则。

欧洲和日本也有不同的3G系统发展短期目标。在欧洲，经历了早期的窄带GSM数据应用后，普遍认为需要一种有质量保证的商用移动数据业务(例如移动视频业务)。与此同时，人口密集的远东地区迫切需要增加更多的无线电频率来提供话音业务。在这一点上，1992年ITU为未来3G系统“IMT-2000”制定的频带是最显然的解决方案。1998年初，ETSI TC-SMG决定选择WCDMA作为其UMTS无线技

术，这对3G发展带来了重要推动。这也获得了日本最大运营商NTT DoCoMo的支持。在核心网技术上也同时达成了共识，就是在GSM核心网技术基础上进行开发。在1998年中，欧洲的ETSI和日本的标准化机构（TTC和ARIB）同意制定一个共同的UMTS标准。在此共识下，建立了3GPP组织，既定的UMTS标准化进程在全球范围内启动。

从UMTS角度来说，3GPP组织就像一把"大伞"，要顾及政治、行业和商业方面的压力，建立起折中的标准，这些压力主要来自于各地的标准化机构。

- ETSI（欧洲电信标准协会）/欧洲。
- ARIB（电波产业协会）/日本。
- CWTS（中国无线通信标准研究组）/中国。
- T1（标准化委员会T1——电信）/美国。
- TTA（电信技术协会）/韩国。
- TTC（电信技术委员会）/日本。

由于这项任务非常艰巨，3GPP成立后立即建立了一个名为OHG（运营商协调小组）的独立组织。3GPP的主要任务是定义并维护UMTS标准，OHG负责寻找那些3GPP内部不能解决的问题的折中方案。这种分工保证了3GPP的工作能按计划进行。

为了保证美国的观点能列入考虑范围，成立了一个独立的3GPP2组织，该组织负责基于IS-95无线技术的标准化工作。3GPP、OHG以及3GPP2的共同目标是建立这样的标准，根据它能实现具有宽带无线接入的全球蜂窝系统。总而言之，有三种不同的方法能通向全球蜂窝系统——3G。表1.1粗略地给出了这些方法及其组成。

表1.1 3G的不同版本及其组成

版 本	无线接入	交 换	2G基础
3G（美国）	WCDMA，EDGE，CDMA2000	IS-41	IS-95，GSM1900，TDMA
3G（欧洲）	WCDMA，GSM，EDGE	高级GSM网络子系统及分组核心	GSM900/1800
3G（日本）	WCDMA	高级GSM网络子系统及分组核心	PDC

当全球性成为现实，3G规范能使表1.1中提到的任何交换系统与任何指定的无线接入部分结合起来，形成一个可运行的3G蜂窝网络。表1.1的第二行是以UMTS著称的欧洲方法，本书将综述其第一个版本。

3GPP最初决定以年度为基础准备规范，第一个规范版本是R99。这个版本具有相当明显的"GSM存在"。从UMTS的角度来看，GSM的存在是非常重要的。首先，UMTS网络必须后向兼容现存的GSM网络；其次，GSM和UMTS网络必须能共同运

营。下一个版本应是“3GPP R00”,但出于修改建议的多样性,将标准化过程计划为两个规范版本,分别是3GPP R4和3GPP R5。3GPP R4定义了UMTS核心网电路交换侧的可选变化,这把用户数据流和相应的控制机制分离。3GPP R5旨在为UMTS网络引入多媒体机制。这一实体就是IMS(IP多媒体子系统),其结构将在第6章中阐述。网络控制也将采用IP和IP上的协议,用户数据流也将主要是基于IP的。换言之,3GPP R5所实现的移动网络将是一个端到端的分组交换蜂窝网络,传输层协议用IP替代在现有电路交换网络中占主要地位的SS7(7号信令系统)。当然了,基于IP的网络也应当支持电路交换业务。3GPP R4/R5也将尽可能地利用新的无线接入技术。3GPP R99中UTRAN(UMTS陆地无线接入网)的基础是WCDMA无线接入。3GPP R4/R5中还集成了另外一种源于GSM的无线接入技术,以创建GERAN(GSM/EDGE无线接入网)作为建立UMTS移动网络的一种选择。

1.2 3G网络结构介绍

3G背后的主要目的是准备一种通用的结构,这种结构可以承载目前和未来的业务。这种结构的设计应能使网络在适应技术改变和发展的同时,不会对使用现有网络结构的现有业务带来不确定性。将接入技术、传输技术、业务技术(连接控制)、用户应用等进行分离可以应付这种迫切的要求。可以用很多方法建立3G网络结构的模型,在此我们介绍一些方法来描述网络的基本结构。在本节中讨论的结构化方法有以下几个。

- 概念化网络模型。
- 结构化网络体系。
- 资源管理体系。
- UMTS承载体系。

1.2.1 概念化网络模型

从上述概念化网络模型的观点来看,根据业务属性、协议结构和物理单元,整个网络结构可以分成多个子系统。就业务属性而言,3G网络由两个主要的域组成,PS(packet-switched,分组交换)域和CS(circuit-switched,电路交换)域。根据3GPP标准TR21.905,域指最高等级的物理实体组和定义在域之间的接口(参考点)。这些接口及其定义确切描述了域之间的通信。

从协议结构和它们的功能来看,3G网络可以分成两层:接入层和非接入层。所谓层是指协议分组的方式,这些协议与一个或多个域提供的业务的某个方面有关(参见3GPP标准TR21.905)。因此,接入层包含的协议处理UE(User Equipment,用户设备)和接入网之间活动。非接入层包含的协议处理UE和核心网(CS/PS域)之间的活动。有关层和协议的更多信息请参见本书的第10章。

图 1.2 中的"归属网络"部分维护静态的用户及安全信息。服务网络是核心网的一部分加上为本地用户提供核心网功能的域。转接网络是核心网的一部分,位于服务网络和远程网络之间的通信路径上。对于给定的呼叫,如果远程网络和主叫 UE 处在同一网络中,则不需要转接网络。

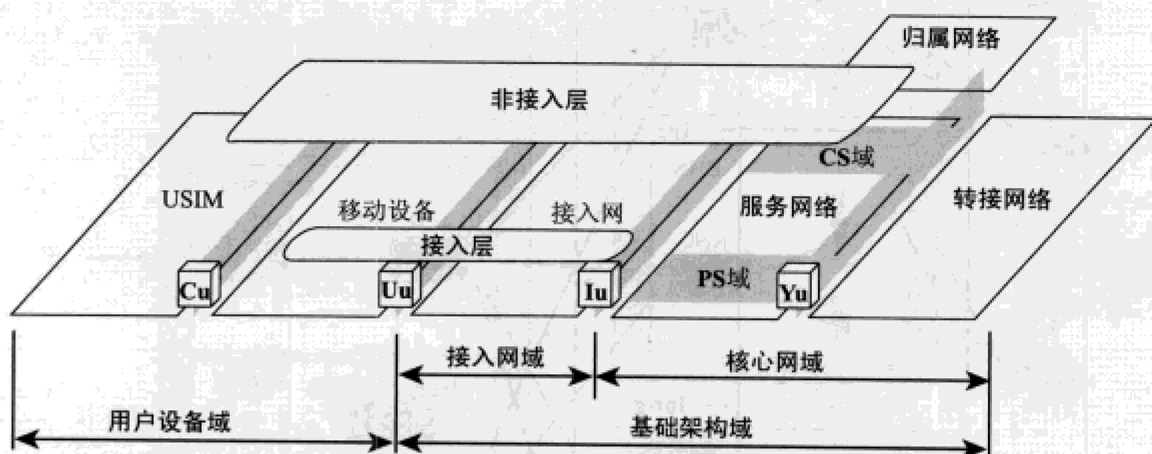


图 1.2 UMTS 结构——概念模型

1.2.2 结构化网络体系

本书主要从结构化网络结构的角度展开,如图 1.3 所示。在 UMTS 中,GSM 技术起着背景支撑的重要作用,UMTS 实际上就是要复用 GSM 中一切合理的东西。例如非接入层中使用的某些过程原则上复用了 GSM,只是会做一些必要的修正。

3G 的系统终端称为 UE,它包括两个独立的部分,ME(Mobile Equipment,移动设备)和 USIM(UMTS Service Identity Module,UMTS 业务识别模块)。

控制宽带无线接入的新子系统有不同的名称,取决于所使用的具体无线技术类型。通用的名称是无线接入网络(Radio Access Network,RAN)。特别谈及带有 WCDMA 无线接入的 UMTS 时,称为 UTRAN 或者 UTRA。UMTS 中包括的另一种类型的 RAN 是 GERAN。虽然 GERAN 是将来可能会用到的一种无线接入选择,但它及其定义并不是 3GPP R99 的一部分。在 3GPP R4 和 3GPP R5 中 GERAN 标准及其与 UTRAN 的协调已经完成。

UTRAN 又被分成若干 RNS(Radio Network Subsystem,无线网络子系统)。每个 RNS 由一组无线单元和相关的控制单元组成。UTRAN 中的无线单元是节点 B,也就是本书以后将提到的 BS(Base Station,基站),控制单元是 RNC(Radio Network Controller,无线网络控制器)。RNS 之间通过接入网内部接口 Iur 互连。这一结构及其优点将在本书的第 5 章进行详细阐述。

本书对图 1.3 中的另一种接入网 GERAN 不做详细介绍。感兴趣的读者可参考 Halonen 等的著作。

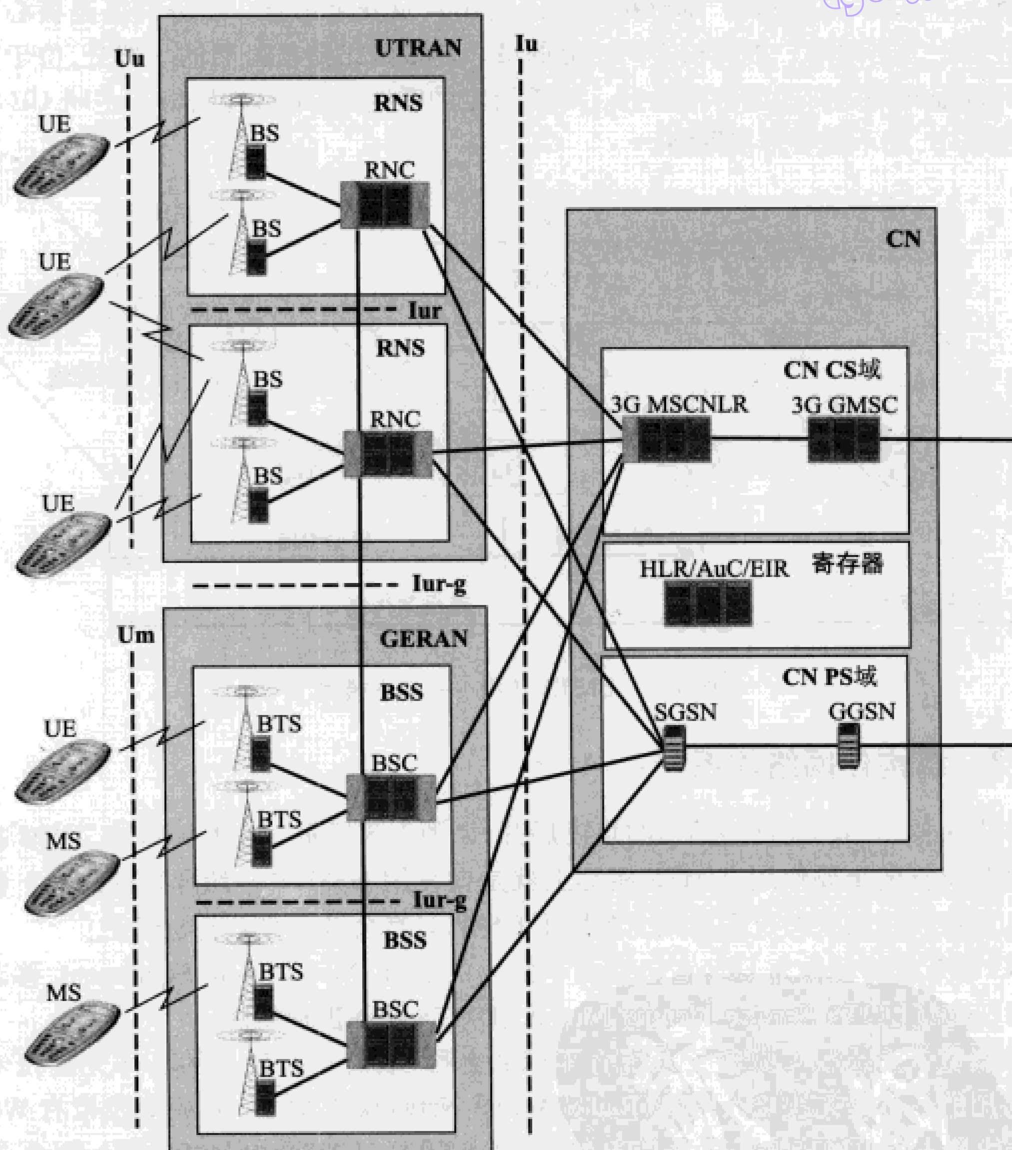


图 1.3　UMTS 网络体系——网络单元及其在用户数据传输时的连接

CN(核心网)这个词覆盖了交换和用户控制所需要的所有网络单元。在早期的 UMTS 中,CN 中的部分单元直接继承自 GSM,并针对 UMTS 进行了修订。后来,随着传输技术的改进,CN 的内部结构也有了显著变化。CN 包含了图 1.3 中的 CS 域和 PS 域。UMTS 核心网的配置选择和各种单元将在本书的第 6 章详细讨论。

图 1.3 中的"寄存器"部分和之前 3G 网络概念模型的归属网络相同。这部分维护静态的用户和安全信息。关于寄存器的内容也将在第 6 章中进行详细的阐述。

图 1.3 还示出了 UMTS 中的主要开放接口。UE 和 UTRAN 之间的开放接口是 Uu,在 UMTS 中通过 WCDMA 技术来实现。第 3 章和第 4 章将对 WCDMA 做更多一般性介绍。在 GERAN 侧的等价开放接口为 Um。另一个主要的开放接口是 Iu,它位

于 UTRAN/GERAN 和 CN 之间。

开放接口 Iur 把各个 RNS 分开。与 GSM 相比，Iur 有显著区别，它给系统增添了全新的功能：宏小区分集以及更为有效的无线资源管理和移动性机制。当网络运用了 Iur 接口时，UE 可以通过多个 RNC 和网络连接，每个 RNC 在无线连接期间承担特定的逻辑角色，包括 SRNC（Serving RNC，服务 RNC）、DRNC（Drifting RNC，漂移 RNC）和 CRNC（Controlling RNC，控制 RNC）。CRNC 总体控制 UTRAN 接入点（主要是基站）的逻辑资源。SRNC 负责 UE 和 UTRAN 之间的特定连接，每一个和 UTRAN 有无线连接的 UE 都有一个 SRNC，负责 UE 和 UTRAN 之间的无线连接。SRNC 的主要特点是它还维护到核心网的 Iu 接口。当 UTRAN 和 UE 之间连接的无线资源需要使用其他 RNC 控制而不是 SRNC 本身控制的小区时，就需要 DRNC 发挥其逻辑功能。UTRAN 相关的一般性问题将在本书第 5 章讨论。

接入网之间通过 Iur-g 接口连接，Iur-g 用于传递与无线资源管理相关的信息。Iur 和 Iur-g 的不同之处在于 Iur 既传送信令也传送用户数据，而 Iur-g 只传送信令。

除了图 1.3 中的 CS 和 PS 域外，网络也可能包括其他的域，例如负责多播消息控制的广播消息域。不过本书着重介绍图 1.4 中所示的 UMTS 网络。对于各种不同的 RAN，本书着重于 UTRAN，并突出一些与 UTRAN-GERAN 共存、协作有关的问题。

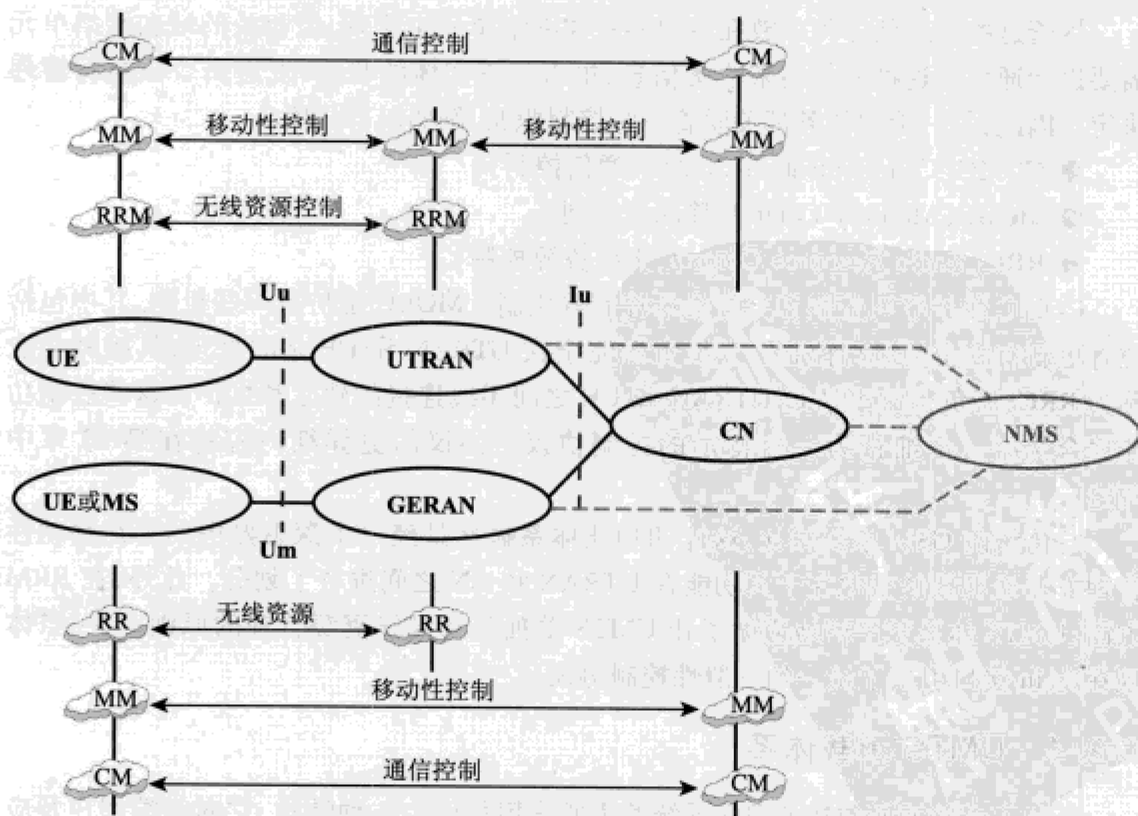


图 1.4　UMTS 网络结构——管理任务和控制功能

1.2.3 资源管理体系

上述以网络单元为中心的结构来自于主要的域之间、最终也是网络单元之间功能的分解和责任的划分。图1.4表示主要功能的划分,这些功能有以下几项。

- CM(Communication Management,通信管理)。
- MM(Mobility Management,移动性管理)。
- RRM(Radio Resource Management,无线资源管理)。

CM包括所有与用户连接管理相关的功能和过程。CM可分为几个子块,比如CS连接中的呼叫处理、PS连接中的会话管理,以及补充业务和短消息业务的处理。MM包括所有移动性和安全所需要的功能和过程,例如连接安全过程和位置更新过程。大部分MM过程出现在核心网及其单元中,但在3G中,PS连接的部分MM功能也在UTRAN中执行。底层的CM和MM的原理将在本书第6章阐述。

RRM是UTRAN用来管理无线资源的算法的集合,例如用来处理无线连接的功率控制、不同类型的切换、系统负载和接纳控制等的算法。RRM是UTRAN的一个有机组成,本书第5章将进一步介绍基本的RRM。第11章将给出一些有关CM、MM和RRM功能的系统实例。

尽管这些管理任务可以放在特定的域和网络单元中实现,但相关的域和网络单元需要进行通信。这种通信用来收集信息、报告远程实体的状态、发送指令以执行管理决定。因此,每一管理任务都关联着一组控制职能,例如以下几项。

- COMC(Communication Control,通信控制)。
- MOBC(Mobility Control,移动性控制)。
- RRC(Radio Resource Control,无线资源控制)。

COMC维护呼叫控制和分组会话控制等机制。MOBC维护着一些机制,其中包括位置更新和安全的执行控制。无线资源完全在UTRAN和UE之间处理,其控制功能称为RRC,所负责的事情是UTRAN和UE之间无线连接的建立和维护。这些控制功能集合又进一步细化为一组特定的控制协议。协议的更详细内容将在第10章中阐述。

与传统的GSM系统相比,这样的功能体系显然是经过了深思熟虑的。在移动性管理方面最明显的变化在于其功能在UTRAN和CN之间进行了划分。此外,在RRM方面,UMTS体系更严格地遵循了让UMTS单独负责无线资源管理的原则,这一点体现在为Iu接口引入了统一的一般性控制协议。

1.2.4 UMTS承载体系

正如本章前面所叙述的,3G系统的主要作用是作为一种结构,它向终端用户及应用提供方法、足够的带宽和质量。这些方法的提供、带宽的分配以及连接质量统称为QoS(Quality of Service,服务质量)。考虑用户之间某个端到端的业务,所用的业务设

定了 QoS 要求,网络的所有环节都必须满足这种要求。UMTS 网络的不同部分通过不同的方法来满足业务的 QoS 要求。

为了对这一问题建立模型,端到端的业务要求分成三个实体:本地承载业务、UMTS 承载业务和外部承载业务。本地承载业务包含了一些如何把终端用户的业务在终端设备和 MT(Mobile Termination,移动终端)之间映射的机制。移动终端是用户设备的一部分,是网络中发送和接收无线传输的终点,使终端设备可以进行无线通信。另外,UMTS 承载业务包含一个把 QoS 分配到由 UTRAN 和 CN 组成的 UMTS/3G 网络中的机制。既然 UMTS 网络自身是和外部网络连接的,终端用户 QoS 请求也必须向其他网络操作,这是外部承载业务所关注的问题。

在 UMTS 网络中,UTRAN 和 CN 的 QoS 操作有所不同。从 CN 的角度来看,UTRAN 虚拟了一个能为终端用户服务提供充分 QoS 的固定承载"幻想",称为无线接入承载业务(radio access bearer service)。在 CN 中,使用的是它自己的承载业务类型,称为"CN 承载业务"。无线接入承载和 CN 承载需要分开是因为在完全不同的环境下必须保证 QoS,而这两种环境都需要有自己的运行机制和协议。例如,CN 承载业务的特性很稳定,因为提供物理连接的骨干承载业务是稳定的。而在 UTRAN 中,无线承载业务将随着时间和 UE 的移动而不断变化,这对 QoS 提出了不同的挑战。这种分离也符合 UMTS 网络的主要体系原则(即整个网络架构独立于无线接入技术)。

图 1.5 所示的结构是从承载和 QoS 的角度建立的网络体系模型。由于 QoS 在 UMTS 中的重要性,QoS 和承载的概念将贯穿本书始终。

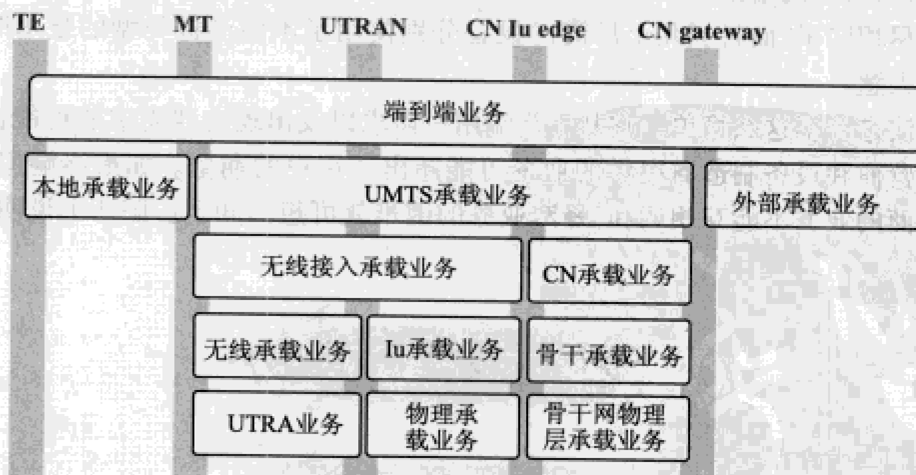


图 1.5 UMTS 承载体系

本书以后的章节将以这些体系为基础,展开对 UMTS 网络及其实施的阐述。

第 2 章
从 GSM 到 UMTS 多址接入的演进

演进是 UMTS(通用移动通信系统)中最常用的术语之一。一般来说,它理解成技术演进(例如,它如何演进、利用什么样的设备以及用何种顺序插入现有的网络)。这种理解在一定程度上是正确的,但是为了理解演进的影响,就要在更广的范围内进行考查。从更高层来看,演进不仅包括网络单元的技术演进也包括网络架构与业务的扩展。这三种类型的演进的同时推进,将成功地实现从 2G 到 3G 的平稳过渡并产生收益。

技术演进意味着网络单元怎样实现和用什么技术实现。这一发展严格遵循通用技术的发展趋势。网络单元的集合形成一个网络,因此理论上网络将相应地进化。在这种情况下,必须注意网络的性能取决于最薄弱的网络单元,而且由于规范中定义的是开放接口,很多网络由多个厂商提供的设备组成。技术演进始终在进行,但到具体厂商就不尽相同了,而且当几个厂商的设备分别使用了不同演进类型的技术时,结果可能不尽人意。

业务演进并不这么简单。它基于终端用户需求以及出现这些需求的可能性,有时候网络运营商和设备制造商提供的业务可能超出了用户的期望。如果终端用户的需求和运营商的业务不能互相调和,蜂窝业务的困难就可想而知了。图 2.1 说明了这三种演进过程。

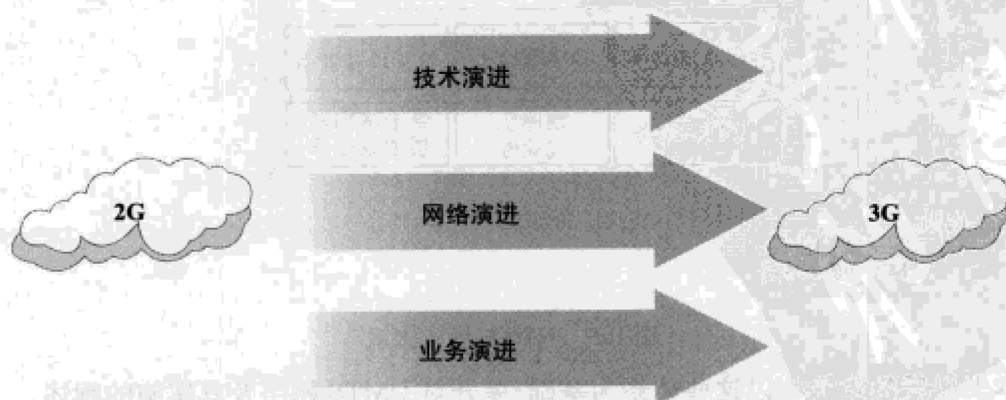


图 2.1　技术、网络和业务演进图

2.1 从模拟到数字

GSM 标准的主要思想是定义了一些开放接口，这些接口决定了 GSM 系统的标准部件。因为这种接口的开放性，运营商可以从不同的 GSM 网络提供商获得不同的网络部件来维护一个 GSM 网络。同时，开放接口严格定义了系统功能怎样在接口处实现，也决定了哪些功能需要由接口两端的网络单元在内部实现。

运行模拟移动网的经验表明，在系统中进行集中智能控制会生成大量负载，因此降低了整个系统的性能。这就是 GSM 标准原则上在整个网络采用分布式智能控制的原因。上述的开放式接口会部署在正确的位置，其实现既自然，技术上又合理。

从 GSM 网络的角度看，这种分散式智能控制通过把整个网络分成以下四个相互独立的子系统来实现。如图 2.2 所示。

- NSS（网络子系统）。
- BSS（基站子系统）。
- NMS（网管子系统）。
- MS（移动台）。

为呼叫建立的实际网络由 NSS、BSS 和 MS 三部分组成。BSS 是网络中负责无线通道控制的部分。每个呼叫都经由 BSS 连接。NSS 是网络中负责呼叫控制功能的单元，每个呼叫都经由 NSS 连接。NMS 是网络中与运行和维护相关的部分，同样也是整个网络控制的组成部分。网络运营商通过 NMS 观察和维护网络的质量和服务。开放式接口位于 MS 和 BSS（Um 接口）之间以及 BSS 和 NSS（A 接口）之间。Um 接口实际上与 ISDN（综合业务数字网）的终端接口 U 非常相似，它实现非常相似的系统功能，同时也采用了窄带 ISDN 中的低层信令。U 后面的小写字母“m”代表“modified”（修正的）。曾经期望 NMS 和 NSS/BSS 之间的接口也是开放的，但它的标准没有及时出台，这就是每个设备制造商使用各自的方法实现 NMS 接口的原因。

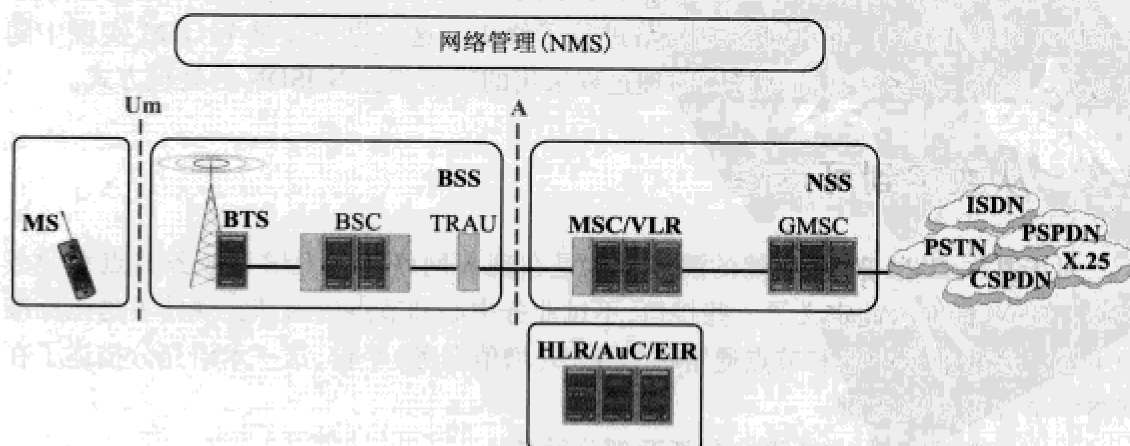


图 2.2 基本 GSM 网络和它的子系统

MS 是终端设备和用户业务识别模块的结合体。所以,终端设备称为 ME(移动设备),而用户数据存储在单独的模块中,称为业务识别模块(SIM)。因此,ME + SIM = MS。注意 SIM 正式的意思是用户识别模块。我们更愿意说成是"业务识别模块",因为它能更好地描述 SIM 的功能。

BSC(基站控制器)是 BSS 的核心网络单元,它控制着无线网络。这说明 BSC 的主要功能有以下方面:维护面向 MS 的无线连接和面向 NSS 的地面连接。BTS(基站收发台)是维护空中接口(Um 接口)的网络单元,它负责空中接口的信令、加密和语音处理。此处语音处理指的是 BTS 为保证 MS 和 BTS 之间的无差错连接而做的各种操作。编码转换和 TRAU(速率适配单元)是 BSS 的一部分,负责语音编码的转换(例如,将语音从一种数字编码格式转换成另外一种或反之)。

从呼叫控制来看,MSC(移动业务交换中心)是 NSS 的主要单元。MSC 负责呼叫控制、BSS 控制功能、互操作功能、计费、统计、面向 BSS 的接口信令和与外部网络(PSTN/ISDN/分组数据网)的接口。从功能上说,MSC 可分成两部分,尽管这两部分功能有可能在同一个硬件上。服务的 MSC/VLR 是维护 BSS 连接、移动性管理和互操作的单元。GMSC(网关移动业务交换中心)单元参与移动性管理、通信管理和与其他网络的连接。HLR(归属位置寄存器)是永久存储所有用户信息的地方。HLR 也提供用户制定的固定路由信息。HLR 的主要功能是用户数据和业务处理、统计和移动性管理。VLR(访问位置寄存器)为所有变量和函数提供本地存储,这些信息用于处理 VLR 相关区域中移动用户发出的和接收的呼叫。只要移动用户访问该区域,用户相关信息将会一直存储在 VLR 中。VLR 的主要功能是用户数据、业务处理和移动性管理。AuC(鉴权中心)和 EIR(设备识别寄存器)是负责安全相关事宜的 NSS 网络单元。AuC 与 VLR 一起维护用户身份相关的安全信息。EIR 与 VLR 一起维护移动设备认证(硬件)相关的安全信息。

从业务上说,1G 与 2G 最显著的区别是出现了数据传输的可能性。基本 GSM 可在网络和终端之间提供 9.6kbit/s 的对称数据链路。基本 GSM 的业务包直接采用 N-ISDN(窄带 ISDN),并针对移动网络进行了修正。这一思想在整个 GSM 实现中随处可见。例如,许多消息流和接口处理过程采用的就是相应 N-ISDN 的处理方式。

2.2 从数字到可达性

对于基本 GSM 来说,自然的演进步骤是在现有网络架构上增加业务节点和业务中心。GSM 标准为此定义了一些接口,不过业务中心和节点的内部实现并不是该标准的主题。这些业务中心和节点通常称为 VAS(增值业务)平台,这一术语充分描述了在网络中增加设备的关键。

一个典型的小型 VAS 平台包括两部分设备。

- SMSC(短消息服务中心)。

● VMS(话音邮件系统)。

从技术上来说,VSA 平台(图 2.3)设备相对简单,用于提供特定类型的服务。它使用面向 GSM 网络的标准接口,但不一定有面向其他网络的外部接口。

从业务演进来看,VAS 是通过业务或者业务的部分裁剪产生利润所迈出的第一步。这种意义下巨大的成功故事就是 SMS,在起初的设计中,短消息业务只是 GSM 系统一个很小的附加内容。今天,短消息业务在 GSM 用户中极其流行。

基本 GSM 和 VAS 最初的打算是“为大众提供大量服务”,不过,由于终端用户需要更加个性化的服务。为了实现这一点,IN(智能网)的概念融入了 GSM 网络。技术上说,为了增加智能网的功能,交换网络单元将有很大的改变;此外,IN 平台自身就是一个相对复杂的实体。IN 使业务演进朝着个性化迈出了一大步(为个人提供大量服务);更进一步说,采用 IN 使运营商能够更加安全地实施商业策略(例如,预付费用户大都是靠 IN 技术实现的)。

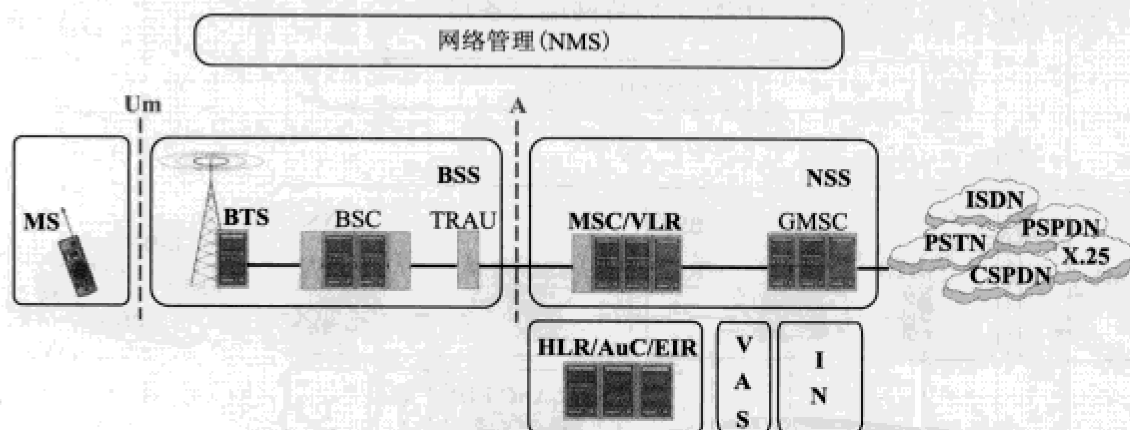


图 2.3　增值业务平台

IN 作为一项技术来源于 PSTN(公共交换电话网),因而并不能满足所有移动网络的需求。所以,IN 最初的概念又被增强并作为 CAMEL(移动网络定制应用增强逻辑)引入。CAMAL 消除了 IN 的缺点,例如 IN 不能很好地支持移动性业务。

2.3　向分组和高速发展

起初,GSM 用户可以使用 9.6kbit/s 的 CS(电路交换)对称“管道”进行数据传输。由于因特网和电子报文对移动数据传输带来了很大压力,GSM 系统最早制定标准时低估了这种发展趋势。为了缓解这种情况,GSM 系统在很多方面进行了增强。首先是信道编码最优化,使有效比特速率从 9.6kbit/s 增加到约 14kbit/s。基次,为了提高空中接口的数据传输能力,可以同时使用几条业务信道。这种方法称为 HSCSD(高速电路交换数据)。在最好的环境下,HSCSD 用户可达到 40kbit/s ~ 50kbit/s 的数据传输速率。从技术上来看,这一解决方案非常简单,但缺点是浪费了资源,而且某些终端用户

可能会对这种功能的资费标准不满,HSCSD的应用严重依赖于运营商的定价。另一个问题是,实际上多数的数据传输是不对称的,从终端到网络方向(上行链路)的传输速率一般非常低,而反方向(下行链路)的传输速率则较高。

CS对称的Um接口对于数据链路来说并不是最有可能的接入媒介。再考虑到主要数据业务在自然情况下是PS(分组交换)的,那么GSM的"升级"就需要做更多的事情,才能使它适用于更高效的数据传输。解决方法是采用GPRS(通用分组无线业务)。GPRS需要新增两个特定移动网络业务节点:SGSC(服务GPRS支持节点)和GGSN(网关GPRS支持节点)。利用这些节点,MS就能够通过GSM网络形成到外部分组数据网(因特网)的PS连接。

图2.4是利用基本GSM实现GPRS网络的示意图。注意,全功能的GPRS网络还需要其他设备,例如出于安全原因需要防火墙、GPRS网络路由查询需要DNS(域名服务器)、地址分配需要DHCP(动态主机配置协议)服务等等。这些设备并不是专门针对移动的设备,它们的功能与传统的因特网端设备相同。

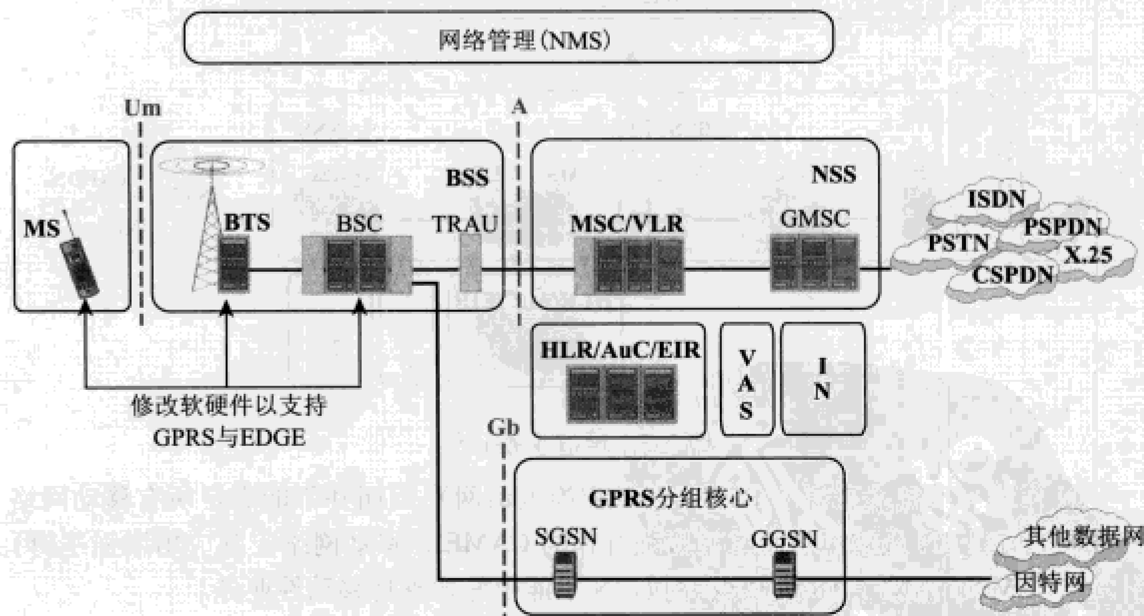


图2.4 通用分组无线业务(示意图)

GPRS具有在必要时可以使用不对称连接的潜能,这样做能更好地利用网络资源。GPRS给IP(因特网协议)带来了移动性,使因特网更接近蜂窝用户,但它并不是一个完整的IP移动解决方案。从业务来看,GPRS开创了传统CS业务向GPRS转变的发展道路,因为这些业务原本就更适合PS连接。一个例子就是WAP(无线应用协议),使用GPRS才充分发掘出它的潜力。此外,GSM最大的杀手级业务(即SMS)在GPRS连接上传输时表现更佳。

应用PS连接时,服务质量(QoS)就成了非常重要的问题。GPRS理论上支持QoS,但实际上并非如此。原因在于GPRS业务在GSM网络中总是处于次优先级:它

使用 Um 接口中另外的未被使用资源。由于未用资源的数量不可预知,所以就不能保证 GPRS 数据在特定带宽上连续传输,因此 QoS 也不能保证。有一些方法能避免这一问题。例如,最经济的方法是为每个小区中留出一个无线信道专供 GPRS 使用。这可以使运营商为特定小区中的移动用户至少保证一定的 GPRS 容量。尽管如此,这种方法还是不能有效解决 QoS 问题。它只是缓解了问题,提高了用户密集的小区中获得 GPRS 服务的可能性。

在这个演进链中,GSM 空中接口用的是传统的 GSM 调制;传输数据的其他方法或者是 CS(HSCSD),或者是 PS(GPRS)服务。使用 GPRS 时,分组数据的传输速率开始成为一个问题,尤其是下行链路方向。通过采用全新的空中接口调制技术,八进制相移键控(8PSK,一个空中接口符号载有 3bit 信息组合),空中接口的比特速率得到显著提高。当这一技术与非常成熟的信道编码技术联合使用时,能够达到 48kbit/s 的数据速率,而常规 GSM 只能达到每个信道 9.6kbit/s 的速率,其空中接口的一个符号只携带一个比特信息。这些技术演进称为“增强数据速率的全球/GSM 演进”(EDGE)。

使用 EDGE 的首要目标是提高分组数据传输速率。这就是 EDGE 在市场上经常作为 E-GPRS(增强版 GPRS)推出的原因。实现 EDGE 需要网络做相应改变,特别是传送机制和发送拓扑,因为基本 GSM 中 BSS 可用的比特速率不够。当运营商增加站台密度并同时启动 EDGE 技术时,这一问题将更明显。有了这两个调整,才能提高每终端用户的平均比特速率,网络不调整时,传输量受处理能力所限。

当 EDGE 实现在 BSS 内外,称为 GERAN(GSM/EDGE 无线接入网)。依靠所引入的信道编码和 8PSK 调制,理论上 GPRS 终端能达到 384kbit/s 的数据传输速率。达到这个速率需要 GPRS 终端占用 8 个空中接口时隙,并采用最高的信道编码,这样数据速率可以达到 8×48kbit/s = 384kbit/s。必须指出的是,市场上兼容 EDGE 的终端达不到这一速率,商用终端同时只能最多使用四个信道。

从网络演进的观点来看,EDGE 通常有它的优点和缺点。优点是达到了一定的数据速率,接近 UMTS 市区覆盖要求。缺点是所提供的数据速率并不一定能在整个小区中可用。如果 EDGE 提供完全的覆盖,小区数量将会急剧增加。换句话说,EDGE 在有些情况下可能是很昂贵的方法。现在把 EDGE 的未来看成是一种补充技术,用来改善基于 WCDMA(宽带码分多址接入)的 UTRAN 和基于 GSM 的 GERAN 之间的互通,这两个接入网组成了 UMTS 网络定义的基本接入方法。

2.4 3GPP R99

3G 引入了新的无线接入方法,即 WCDMA。WCDMA 及其各种版本是全球性的,因此所有 3G 网络应当允许任何 3G 用户的接入。除了它的全球化特性之外,WCDMA 经过了实验室中深入的研究,表明在一定条件下它比 TDMA(时分多址)有更好的频谱效率,比基于 TDMA 的无线接入更适合分组传输。WCDMA 及其无线接入设备也因此不能与 GSM 设备兼容,所以在网络中部署 WCDMA 时,必须增加两个新的设备:RNC

(无线网络控制器)和BS(基站)。包含这些设备,并且维护WCDMA无线技术的网络部分称为UTRAN。如图2.5所示。

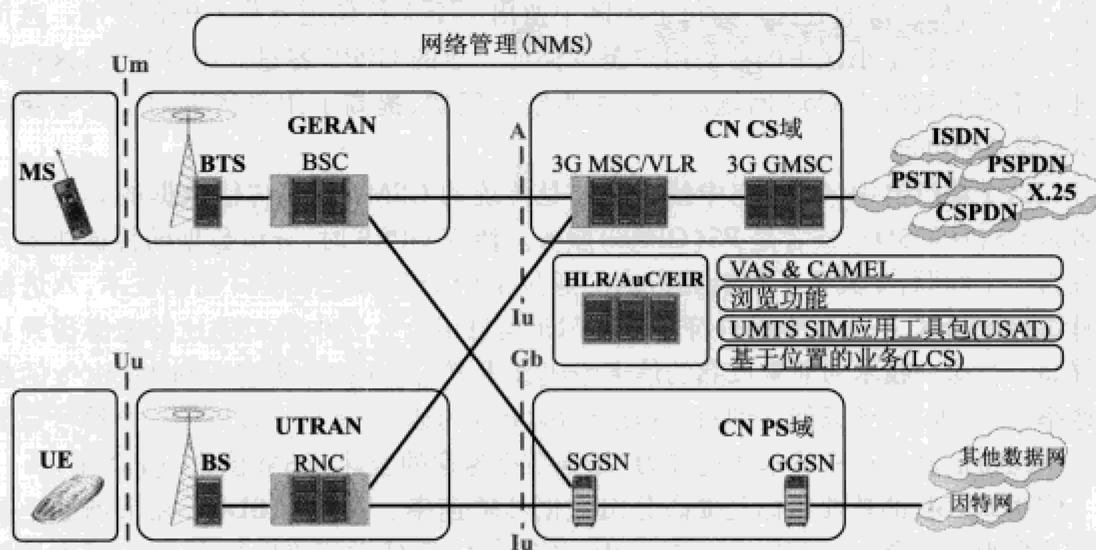


图2.5　3GPP R99上的3G网络实现

另一方面,UMTS的一个关键要求是GSM/UMTS的互操作性,例如系统间切换,即在通信过程中无线接入要从GERAN转换到UTRAN或相反。有两点措施来解决这种互操作问题。首先是对GSM空中接口进行修改,使它能在下行链路中广播关于WCDMA无线网络的系统信息。WCDMA无线接入网当然也能在下列链路中广播周边GSM网络的系统信息。其次是最小化运营成本,3GPP规范中引入了进行互操作功能的可能性,它使演进的2G MSC/VLR能处理宽带无线接入UTRAN。

IN平台目前提供的能力从业务来看已经足够了。IN的概念是直接从PSTN/ISDN网络继承过来的,因此涉及移动应用时会有一些不足。标准IN的主要问题是不能在网间传输业务信息。换句话说,用户只有在归属网络中使用基于IN的业务时,才能正常工作。前面已经指出,CAMEL能解决这一问题,它能在网间传输业务信息。CAMEL在未来3G实现中的作用将会大大增加,事实上,几乎每个3G网络上的通信都会在某种程度上涉及CAMEL。

在3GPP R99运行中,WCDMA无线接入网内的传输连接是通过在物理传输媒质上采用ATM(异步传输模式)来实现的。预标准化项目FRAMES(1996—1998)深入讨论了网络中是否使用ATM的问题。最终结论倾向使用ATM,原因有以下两点:

- ATM的信元和净荷相对很小。其优点是对信息缓存的要求降低。缓存太大时,期望时延很容易增加,缓存器的静态负载也会增加。必须注意,缓存及其导致的时延对实时业务的QoS需求有负面影响。
- 也考虑过另一个办法,即IP(尤其是IPv4版本)。但是IPv4有非常严重的缺点,地址空间有限并缺少QoS保障。而ATM及其比特速率等级能很好匹配

QoS 需求。所以产生了 ATM 与 IP 融合的结果(针对分组业务),将 IP 应用于 ATM 的顶层。这一解决方案融合了两种协议的优点:IP 保证了与其他网络的连接而 ATM 负责连接质量和路由,从而中和了 IPv4 的缺点。某些网络单元使用固定的 IPv4 地址类型,实际终端使用动态分配的 IPv6 地址,3G 网络兼容该地址。在这种情况下,为使 3G 网络适应其他网络,3G IP 骨干网必须包含 IPv4 <—> IPv6 地址转换功能,因为外网不一定支持 IPv6。

CN(核心网)节点也进行了技术演进。CS 域的单元应能够处理 2G 和 3G 用户。这需要改变 MSC/VLR 和 HLR/AC/EIR。例如 2G 和 3G 在建立连接时的安全机制不相同,现在需要 CS 域单元能够处理它们。PS 域实际上是一个演进的 GPRS 系统。虽然单元名称与 2G 相同,但功能已经不同了。最显著的变化是 SGSN,其功能与 2G 差别很大。在 2G 中,SGSN 主要负责分组连接中的移动性管理(MM)活动。在 3G 中,MM 实体在 RNC 和 SGSN 之间划分。这意味着并不是 UTRAN 中用户引起的每个小区改变对 PS 域都必须可见,但 RNC 处理这些情况。

按 3GPP R99 实现的 3G 网络提供与 GSMPhase2 + 相同的业务。就是说,所有相同的补充业务仍然可用,远程业务和承载业务有不同的实现方式,但这对于用户是不可见的。话音呼叫还是话音呼叫,不管它是通过 GSM 业务通道还是使用 3G 带宽。此阶段的 3G 网络还可能提供一些 GSM 中没有的业务,如可视电话、各种流媒体业务,以及基于位置业务的多媒体消息。在此阶段,只要合理并且可以实现,多数业务就会转移或转换到 PS 域。

新的业务需要新的平台来实现。我们从 GSM 和 GPRS 已经引入的 WAP 说起。WAP 有它自己的局限性,它为终端用户提供的内容还没有完全被用户接受。终端的发展为网络中使用更高级的方法提供了可能。不只纯 WAP,终端还使用了网络支持的浏览器功能,同时该浏览器功能也实现了 XML 定义。终端用户把这看作是完全的浏览体验,有彩屏和格式化的文档,很像普通的台式计算机从因特网上得到的那样。

对于 3G 网络为终端用户提供的其他业务来说,这样的浏览功能是一个基石。这一阶段另一个很有吸引力的业务平台是 UMTS SIM 应用工具包(USAT),它能空中处理 SIM 卡。总的来说,业务的个性化是一个非常有趣的事情。这方面的另一个业务分支是发送的内容,取决于终端用户的位置。这种情况下,3G 网络包含一个能使用 LCS 的平台。

2.5 3GPP R4

为了方便,我们说 3GPP R99 是基于 GSM 的,GSM 演进的移动网络包含两个不同的接入网并以可变的速率传输 CS 和 PS 业务。

根据已公布的 3GPP 演进工作,3GPP R4 包含了一些主要的实行项目。从网络

体系来看,最重要的是UTRA频分双工中继器功能、CN协议的IP传输和承载独立CS CN。

与GSM无线接入不同,WCDMA无线接入能更好地扩展覆盖,并能在无线覆盖范围内"转移"容量。但这并不简单,例如,中继器的使用也会对LCS等产生一定的影响。3GPP R4(图2.6)提供了一个转换协议栈的选项,能将传输协议转换成基于IP的。上述第三点,承载独立CS CN能给系统带来可扩展性。传统MSC同时包含连接容量和连接控制容量,但这两种容量不一定能联合。3GPP R4定义了在两个不同节点间划分两种容量的方法。

维护CS连接容量的节点称为CS-MGW(电路交换媒体网关),它负责所有的物理连接的建立。维护连接控制容量的节点称为"MSC服务器"。MSC服务器与CS-MGW是一对多的关系(即一个MSC服务器可能控制多个CS-MGW)。运营商可据此优化网络中用户平面的物理长度。这也有助于向基于IP的传输网过渡。

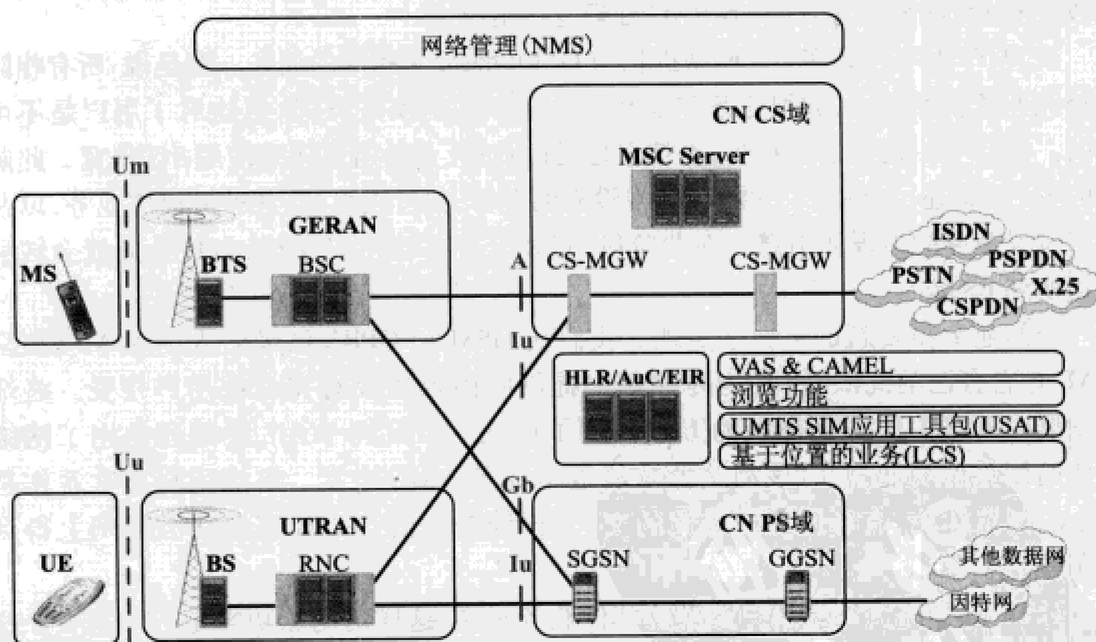


图2.6　3GPP R4实现示意图

2.6　3GPP R5

在3GPP R4之后目标是要实现下面几个主要点。

- 从BS到网络边界网关实现全IP传输。
- 引入IP IMS(多媒体子系统)来启动各种多媒体业务。
- 统一各种接入网和核心网之间的开放接口。
- 使UTRAN空中接口在下行链路中取得更大的容量。

3GPP R5(图2.7)中要实现的项目旨在简化网络结构,统一传输协议环境使得能采用比R3更简明的解决方案。第一主要项,从BS开始的全IP传输目的是为了简化传输网结构。

从业务角度看,IMS将会在R5及以后的实现中起重要作用。IMS是一种独立的系统解决方案,它自身能够利用包括UMTS在内的各种网络。依靠IMS,终端用户能够使用复杂的多媒体和消息业务。IMS体系将在第6章中介绍,第8章将讨论与之相关的业务。

从终端用户的角度看,UMTS的目标是协调网络结构(即终端用户不需要知道他是通过何种接入网使用网络并得到服务的)。为使这一过程尽量平衡,各种接入网必须尽量互相协调。网络中的"协调点"是CN和接入网之间的Iu接口。

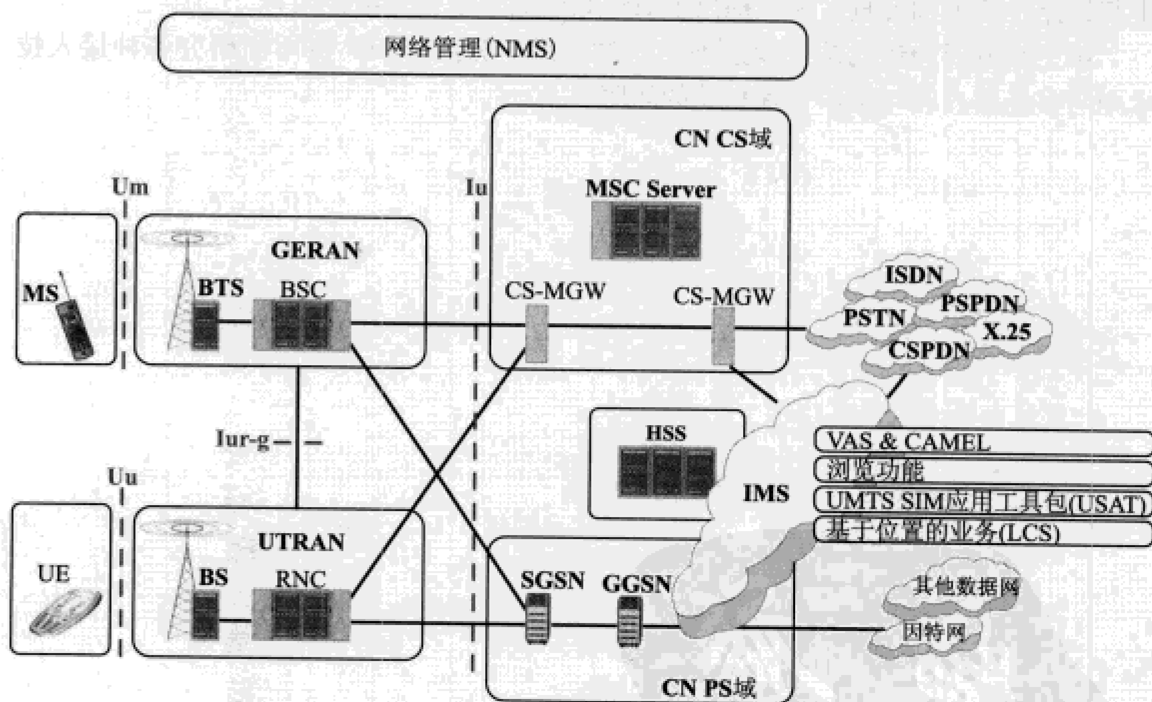


图2.7 3GPP R5示意图

UTRAN从一开始就有Iu接口,而GERAN没有。3GPP R5的主题之一就是让GERAN变成与UTRAN功能相似的网络。通过这些改变,GERAN将工作在Iu模式。为了使终端用户相关的无线功能尽可能平稳过渡,UTRAN和GERAN之间定义了名为Iur-g的接口。Iur-g不传输用户平面,它只是为了信令目的而提供的。

此阶段预期绝大部分使用的业务有非对称特性(即下行链路的负载比上行链路大)。为了在UTRAN中更好地处理这一情况,引入了与UTRAN无线信道相关的一系列改变,总称为HSDPA(高速下行分组接入)。它影响在UTRAN的无线信道、BS和传输信道管理。第4章中将对HSDPA进行更详细的讨论。

2.7 后3GPP R5的趋势

3GPP R5之后会怎么样?① 这个问题没有确切的答案,但能看到一些趋势。

人们预期,IP会在整个传输网中代替其他技术,同时也将在业务实行、接入和网络控制方面成为关键的方法。换句话说,以某种方式实现的全IP解决方案很可能是3GPP R5之后的主要趋势之一。

在业务方面的预期是,将会出现利用IP的所谓的对称业务,例如有实时图像的交互式视频会议。当这些业务对公众普及时,空中接口容量将会再次变得紧张。3GPP R5中的HSDPA在下行方向增加了容量。为了实现上面提到的对称业务,无线信道的上行链路也要增加容量。为此提出了HSUPA(高速上行分组接入)。

第三个发展趋势就是持续进展的协调问题。为此,3GPP将不断研究各种接入技术中与多址接入和互操作管理相关的问题。

① 3GPP R6于2004年4季度发布,引入了HSUPA、MBMS等特性,改进了IMS,集成了与WLAN的操作。3GPP R7于2007年4季度发布,主要关注延时的减少、改进QoS和诸如VOIP的实时应用,还定义了HSPA+、EDGE、Evolution等。Release8预计于2009年发布,旨在大幅改造UMTS,使之成为全IP网络。——编者注

第二部分

第3章
移动网络结构面临的主要挑战

本章的目的是简要地介绍移动网络结构面临的基本挑战，这样首先可以使读者了解考虑任何无线通信系统的基本结构时各种限制和机遇背后的原因，其次可以使读者大致了解这些问题一般是如何提出的，重点放在UMTS网络。

图3.1给出了移动网络中可能成为网络结构瓶颈的关键部分。无线通信中的基本限制、骨干传送引起的问题、网络管理的作用和必要性、无线频谱的稀缺性等关键因素成为移动网络结构发展的边界条件。要实现最优网络结构，就需要所有这些部分共同演进，并且所有解决方案都要顾及总体结构中的一致协调性。

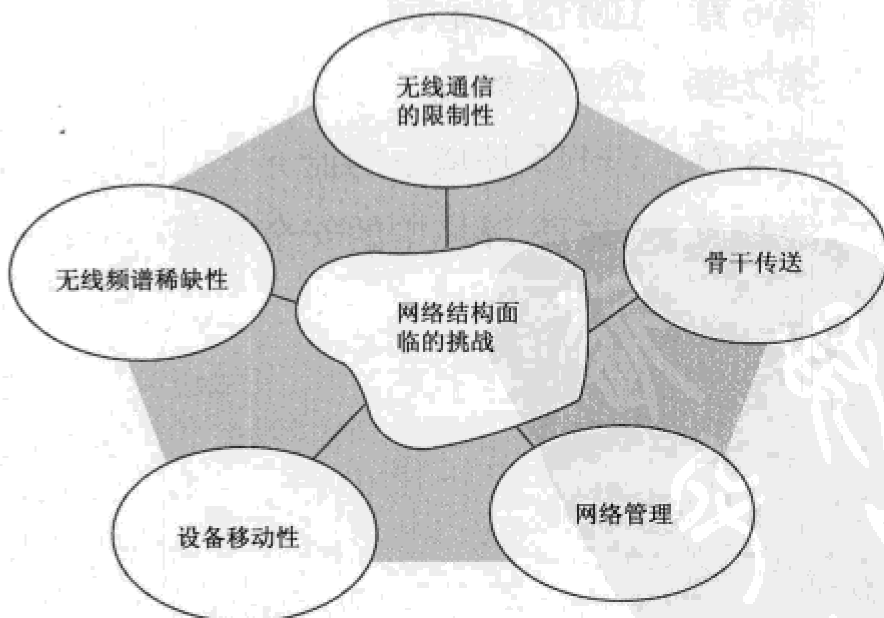


图3.1 移动网络结构设计中的主要挑战

3.1 无线通信的限制

在麦克斯韦于1864年给出了电磁场的基本方程之后，赫兹于1887年实验性地证明了光电之间的关系，无线通信的应用才得以实现。此后，马可尼使用“Hertzian”波来

通信，于1896年发明了无线电报。

无线通信的基本原理是利用无线电波作为传输介质。无线电波是电磁场作用而形成的一种自然现象。在一定条件下，时变电磁场会产生由源向四周辐射的波。这种电磁场源可以是基站或手机之类的发射机。如同其发射源一样，无线电波及其特性也与传播环境密切相关。因此，基于无线电波的通信系统易受环境因素（比如山脉、丘陵、建筑物等大型反射体、大气条件等）的影响。

每个无线通信系统至少由两部分组成，即发射机和接收机。在移动系统中，这两部分也可以集成到一台设备上（即收发器），使之既作为发射机又作为接收机。在任何一个先进的公众移动系统中，基站和手机就是这样的收发器。图3.2示出了一个最简单的无线通信系统，由一个基站和一台手机组成。假定在某特定环境下，基站在某特定时间作为发射机，那么无线信号以光速从基站向移动台传播，手机端接收的信号强度主要取决于手机与基站的距离、波长和通信环境。

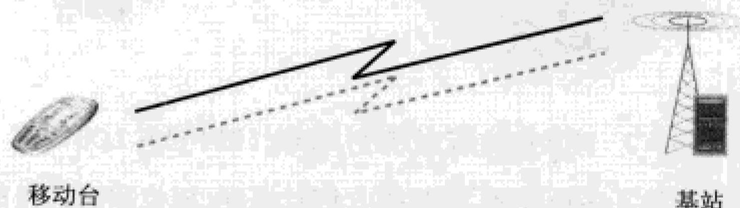


图3.2　无线通信系统的基本组成

妨碍无线电波传播的环境因素既有人造的，也有自然的，如高层建筑、地形和天气等。当信号从发射机向接收机传播时，这些因素能影响信号传输的路径、相位和时间。系统参数（如天线高度和波束方向性）自身也会对传播距离、信号强度和衰减产生影响。因此，无线通信本质上就带来一些固有的限制。任何无线通信系统都面临的主要问题包括以下几项。

- 多径传播现象。
- 衰落现象。
- 无线资源稀缺。

在这些问题当中，多径传播也被很多人认为是无线通信的一个优点，因为它使得无线接收机即使在没有视距（LOS）信号的情况下也可以接收到来自基站的信号。尽管如此，多径传播对接收机和发射机结构有特别的要求和限制，加大了系统的复杂性。必须很好地理解上述特性，才能理解无线通信系统的本质。

影响无线传播的因素是极为动态、不可预知和变化多样的。尽管如此，为了能对传播现象建模，有必要对这些因素进行分类和建模，从而使我们能适当处理这些问题。如图3.3所示，从发射机到接收机的传播过程中，除了那些直接发送到接收机的部分（LOS）外，无线电波还要经历反射、绕射和散射。

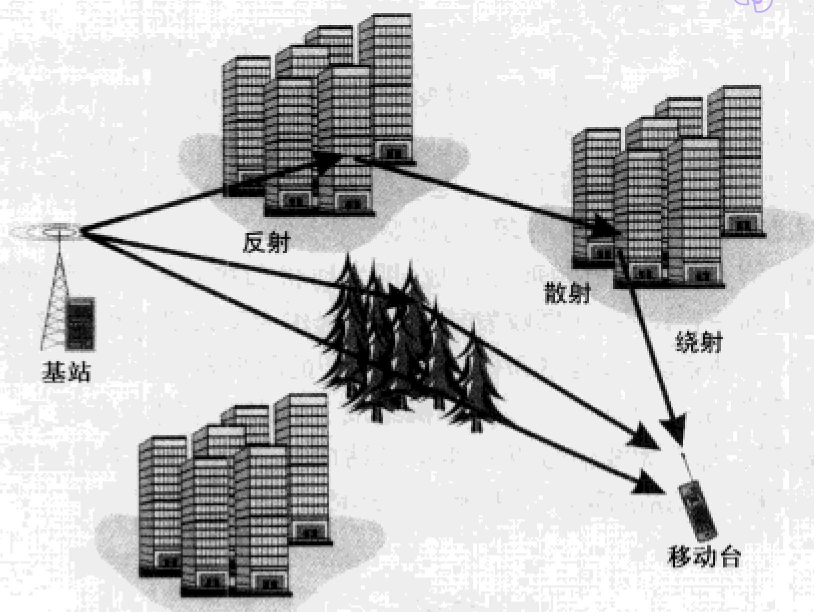


图 3.3　传播机制:反射、散射和绕射(图中已有 LOS)

这些传播机制导致了多径传播,引起接收信号幅度、相位和到达角的波动,称为多径衰落。反射是电磁波遇到相比于波长非常大的障碍物时发生的现象,其结果产生了能被接收机(如移动台或基站)主动捕获的无线电反射波。绕射也称为"阴影",是无线电波遇到不可穿透障碍物的结果。散射则是无线电波遇到与波长大小相同或更小的障碍物的结果。这些现象可以说明,为什么无线电波能在甚至没有 LOS 路径的无线网络环境中传播。

从接收机的角度来看,根据上述传输机制的具体不同,接收信号功率受这些因素或其组合的随机影响。此外,设备的移动性、室内室外覆盖、分层网络结构等对传输环境引入了更复杂的因素,问题也变得更难以处理。

不过,怎样才能预测这些因素对无线信号的最终影响?有不同的方式来描述传播特性对无线信道中信号强度的影响,即链路预算和时间扩散。链路预算的基本思想是测定离开发射机(如基站或移动台)特定距离或位置处期望的信号电平。通过对链路预算建模,可以确定出无线网络的一些基本参数,比如发射功率要求、覆盖范围和电池寿命。通过估计信号的路径损耗可以计算出链路预算。路径损耗的估算可基于自由空间模型,该模型表明,在理想的自由空间模型中,基站和移动台之间的信号强度衰减基本上遵循倒数平方的规律。

由于移动网络环境的差异,不可能预计到所有影响无线信道建模和系统设计的参数。因此,人们提出了一些如 Okumura-Hata 的通用模型,能在某种程度上反映大多数典型情况。但是为了考虑无线信道衰落的全面影响,仅有链路预算是不够的,必须要考虑时间扩散造成的多径传播的影响。这一点可以通过估计发送信号到达接收机时

的不同副本的传输延迟变化来完成。

典型的衰落过程如图 3.4 所示。任何一个衰落过程曲线都有两种不同的简单形状,下降处意味着信号强度的衰落,上升处意味着不期望出现的干扰。因此,利用这些简单曲线的组合可以估计出衰落过程的包络,并能确定出相应的弥补行为来使信号波动控制在预期的均值左右。

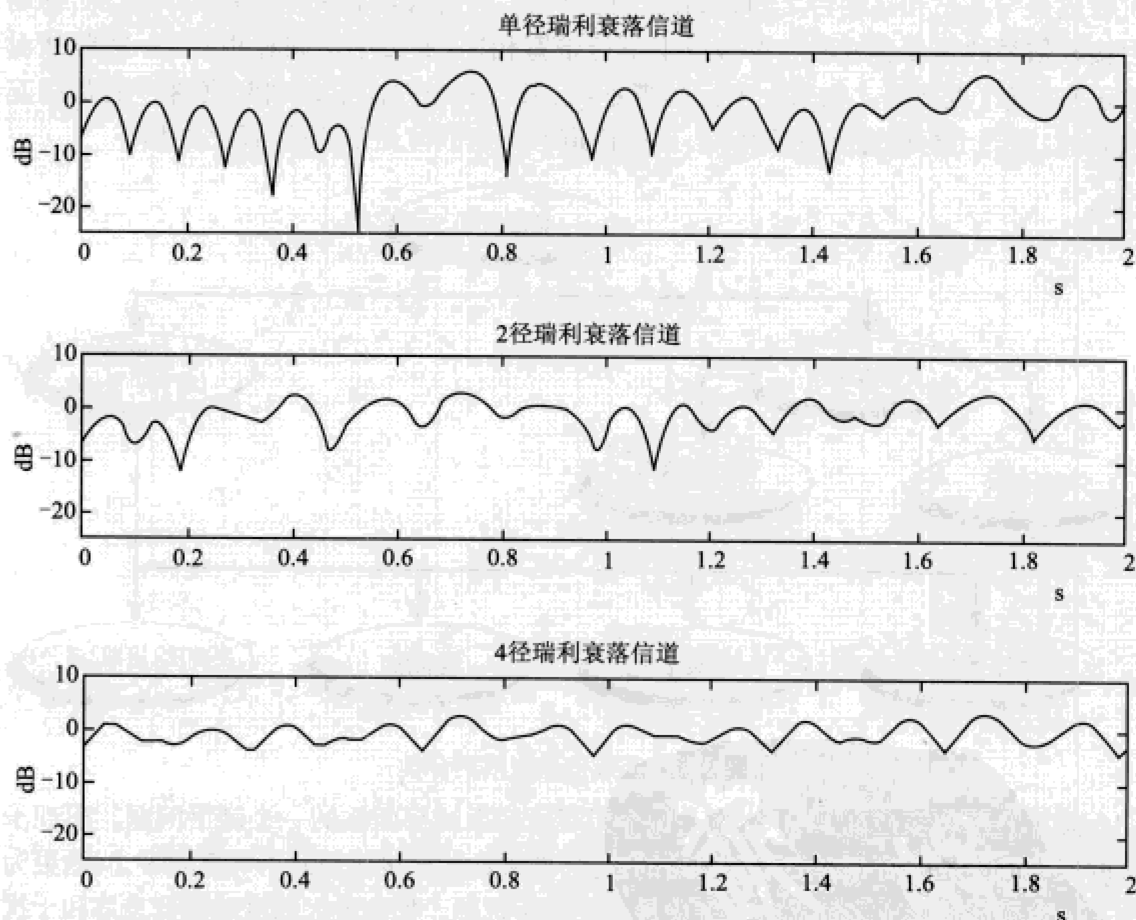


图 3.4 单径、2 径和 4 径信道中典型的信号功率衰落

图 3.5 示出了一些主要的衰落类型,根据不同的环境,它们可以在任意无线网络中以不同的方式出现。无线信道衰落主要包括大尺度和小尺度衰落。前者代表设备在基站和移动台之间跨地域移动所造成的平均信号功率衰减或者路径损耗。另一方面,小尺度衰落则是基站和移动台之间信号幅度和相位快速变化的结果。根据反射路径中的 NLOS 或 LOS 特性,小尺度衰落也称为瑞利衰落或莱斯衰落。小尺度衰落还可进一步分为频率选择性衰落、平衰落、快衰落和慢衰落。无线信道应按所经历的衰落类型来建模。

总体上来说,移动无线信道经历的信号衰落很可能由无 LOS 的瑞利衰落构成,这使得信道更难处理。结果从各个方向到达移动台的信号存在不同的延迟,引起不同支

路信号传输之间有显著的相位差。另外,无线信道的衰落与移动台的物理位置和移动密切相关。既使移动台物理位置或移动速度很小的变化也可能导致各支路信号的相位差,因此移动台在无线网络中的移动可能导致快衰落,它会严重影响无线信号的质量,从而对无线网络的规划和优化提出严格的要求。

假设基站以固定的功率向移动台发送信号,那么衰落对基站发送信号强度的影响可看成是与基站和移动台之间距离的反比函数。随着移动台和基站的距离增加,移动台接收信号的强度会减弱。再假设上下行带宽相同,那么平均路径损耗(一般服从对数正态分布)也相同。如果上下行频带不同,那么两个方向上的瑞利衰落一般是相互独立的,即当上行信道处在衰落时,下行信道不一定同时处于衰落,反之亦然。

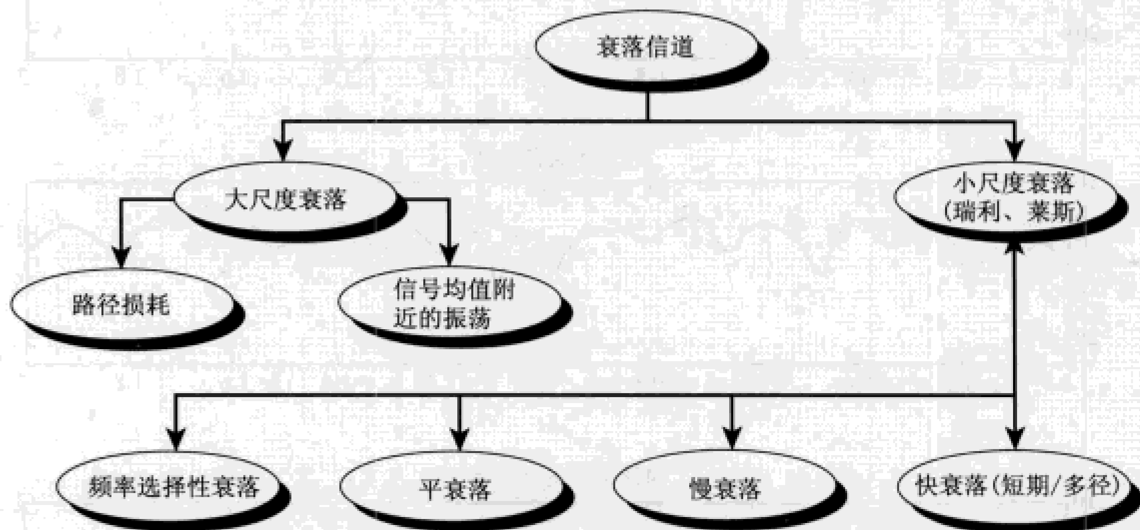


图3.5　无线信道衰落的分类

除了衰落和多径现象,干扰也是每个无线通信系统都面临的一个棘手问题。出现干扰的根本原因是同时存在多个到基站的连接,如果这些连接使用共用共享频带,问题更为严重。这可能是形成多址无线系统中最主要的干扰源。如何最大限度地降低衰落和干扰的影响并优化稀缺频谱资源的使用与诸多因素密切相关,包括网络规划、使用的无线接入技术、控制无线资源的算法、蜂窝概念、调制技术、先进的天线技术等等。因此,在进一步介绍无线系统中的干扰问题之前,我们先来介绍蜂窝系统的概念。路径损耗、衰落和干扰能造成无线系统容量的下降,蜂窝是缓解这种问题的一种基本解决方案。

3.2　蜂窝无线通信原理

本章前面提到的这种简单的无线通信系统不能为大量的终端用户提供接入业务,网络建成后将迅速面临容量限制的问题。我们先根据无线通信的基本特点来找出这种简单系统所存在的基本问题。

首先,公众无线通信为了提供双向同时的通信必须是双工的通信,因此通过广播信息等方式来提供这些业务是不切实际的。另外,接收端的信号强度会随着发射机和接收机之间距离的增加而减弱,使远离发射机的区域内 QoS(服务质量)不可接受。其次,每一个发射机只能够向同时呼叫的终端用户提供有限数量的无线连接(信道)。因此,除了调整系统结构来去掉这些限制,别无他法。

一种非常基本的架构解决方案就是蜂窝的概念。它的主要思想很简单。假定我们正在为一个有上百万移动用户的大型城市规划一个无线网络。蜂窝的思想,是把整个大分域细分为很多子区域,称为小区。每个小区有它自己的基站,通过发射低功率的信号能容纳一定数量的同时通信用户。图 3.6 给出了一个 7 小区簇蜂窝网络的实例。

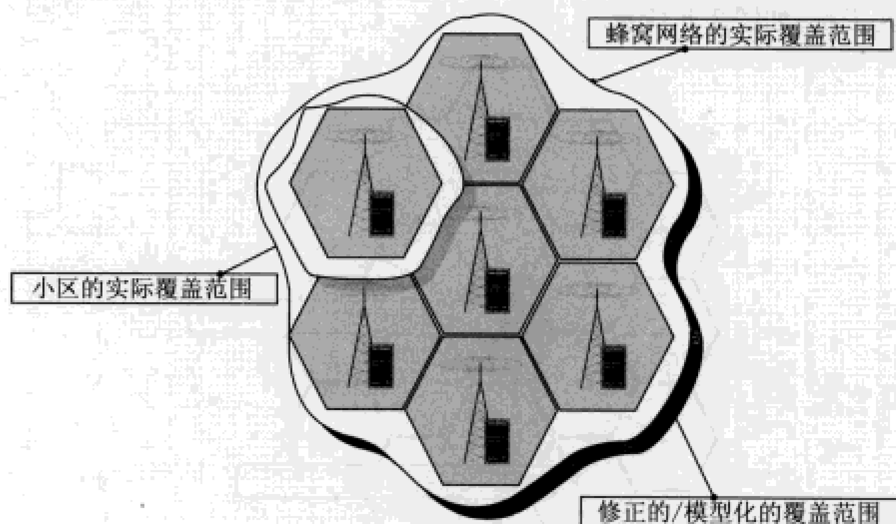


图 3.6 蜂窝网络中的一个小区簇

无线通信的特性和蜂窝的概念是当今移动网络架构的基本出发点。图 3.7 示出了基于蜂窝概念的无线网络的基本结构。如图所示,任何先进的蜂窝系统的基本结构都包括基站、交换网以及提供骨干传输的固网功能实体。

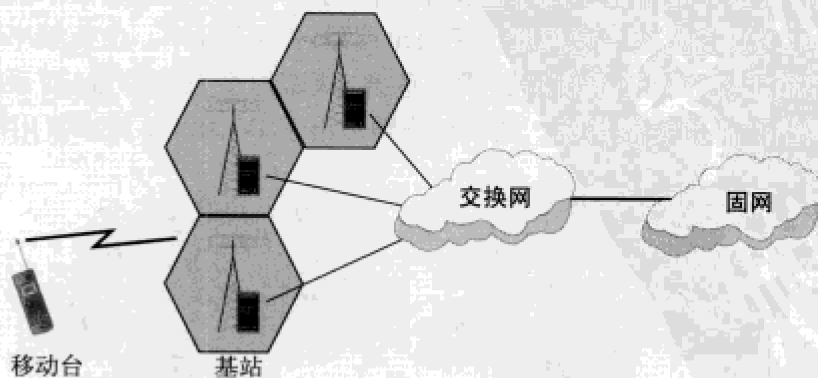


图 3.7 蜂窝网络的简化结构

蜂窝方案解决了无线系统中容量限制这个基本问题，但它也遇到了新的问题，如下所述。

- 蜂窝结构造成的干扰，包括小区间和小区内干扰。
- 移动性造成的问题。
- 每个小区内的无线资源稀缺性。

假定蜂窝系统中异步的用户共享同一无线带宽，每一覆盖区域或小区由同一无线基站服务，那么每个基站不仅会受到本小区的移动台的干扰，还会受到附近小区的终端和基站的干扰。按干扰的来源可分为小区内干扰（同信道干扰）、小区间干扰（邻小区干扰）和热噪声干扰。因此，为了克服终端收到的总干扰，必须要分别研究本小区干扰和邻小区干扰，如图3.8所示。

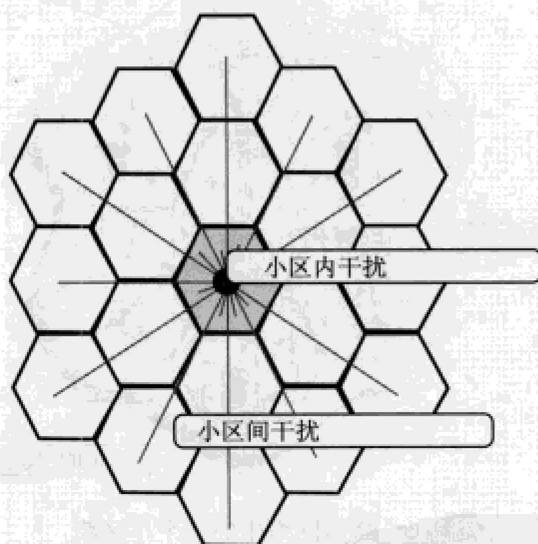


图3.8　蜂窝网络中的小区间干扰与小区内干扰

为了减少信道干扰（包括蜂窝网络中多径和路径损耗问题），蜂窝系统可以采用频率复用技术，它使每个簇中的不同小区使用不同的频率。频率复用因子因而成为蜂窝网的一个基本参数，它能在一定程度上反映出网络的频谱效率。优化频率复用因子可以大大降低邻道干扰和同道干扰所造成的危害，从而提高系统容量，而系统容量是衡量公众无线网络性能的关键指标。图3.9分别示出了1-7和1-1频率复用模式。

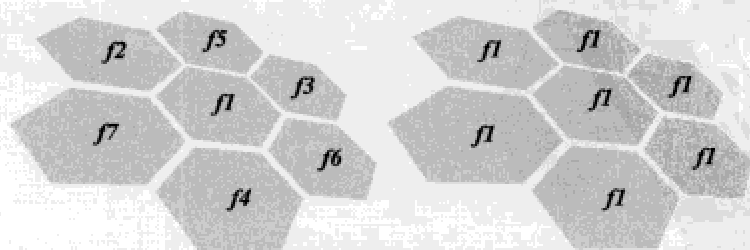


图3.9　频率复用模式的例子，$FR=7$ 和 $FR=1$

蜂窝的思想增加了无线系统的容量,特别是在频率复用程度很高时。小区越小,无线频谱的使用效率就越高,但由于需要的基站更多,因此系统的成本也更高。蜂窝和频率复用的这种思想还可以进一步通过多层网络设计来加强以提高容量,多层网络包括宏小区、微小区和皮小区。

网络规划的主题就是优化网络结构和频率复用的配置,从而能以低成本的方式提高系统容量,避免增加不必要的基站数量。不过这也意味着网络的主要架构应能支持这样的配置与优化。这种解决方案也对所应用的系统提出了新的要求,例如网络必须要有处理设备移动性及切换控制的功能。

3.3 多址接入技术

蜂窝概念的主要目的是解决容量限制问题,但对于多个用户同时工作的情形,蜂窝自身并不能解决每个小区的容量制约问题。从无线频谱的角度来看,知道如何给多个活动用户分配无线资源是非常重要的。对于各种有大量用户的移动网络来说,无线资源控制已经成为最关键的特征之一。

引入多址接入技术的目的是为多个接入请求进行无线接入分配。各类不同的多址接入方案就是对如何共享可用带宽这个问题的具体回答。它所遇到的主要问题也与无线系统的内在特点相关:即带宽限制、多径衰落、使用了蜂窝思想和频分复用的蜂窝网中其他用户的干扰等。有效使用频率就是要在给定的系统参数下,让固定的带宽容纳尽可能多的活动用户。

为了这一目的,人们已经提出了许多不同的多址技术。模拟蜂窝网中广泛使用的多址方式是 FDMA(Frequency Division Multiple Access,频分多址),系统中每个用户都使用自己的一个或一组频率或信道,如图 3.10 所示。从无线连接数来说,就是 1 个频率 = 1 个用户 = 1 个信道。对于公众移动系统中有限的无线资源来说,这种多址接入技术并不是一种有效的共享方式。

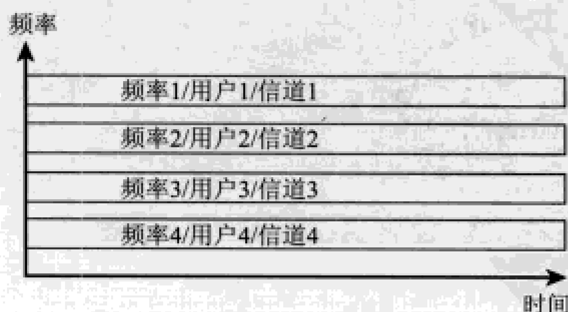


图 3.10 FDMA

因此,在无线通信系统的早期阶段就已经提出了一种更有效的方式,即 TDMA(Time Division Multiple Access,时分多址),它能提高系统容量。TDMA 是 GSM 等 2G

蜂窝系统中最普遍的多址方式。基于TDMA的传输系统也非常广泛,最知名的或许是基于G703标准的PCM(Pulse Code Modulation)传输。

在GSM系统中,给定频率上的用户按时间分割频率,每个用户占用一小段时间(时隙)进行不同的工作。如图3.11所示,时隙频繁重复,产生一个连续连接的效果。这种系统在一个频率上可以有多个用户,用户数就是时隙数,GSM的时隙数是8——同时可以有8个用户使用相同的频率。

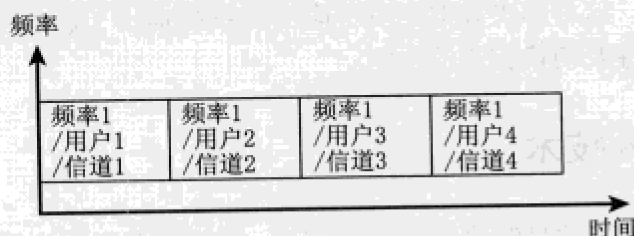


图3.11　TDMA(时分多址)

另一种多址技术是CDMA(码分多址),其目的与FDMA和TDMA类似,但共享频谱的机制完全不同。作为一种基于扩频的无线多址技术,CDMA可能是目前各种通信系统中最为成熟的技术之一(尤其是在UMTS系统中)。

图3.12示出了CDMA分配无线资源的基本做法。与TDMA和FDMA不同,CDMA以码为单元分配无线资源。因此,所有活动用户在同一时间占用同一带宽。每个用户分配有一个或多个码,不同的通信中分配的码也会不同,这些码用于区分小区、信道和用户。CDMA中每个用户同时使用相同的频带,因此没有基于TDMA和FDMA系统中那种时隙和频率分配的概念,而是如下所述。

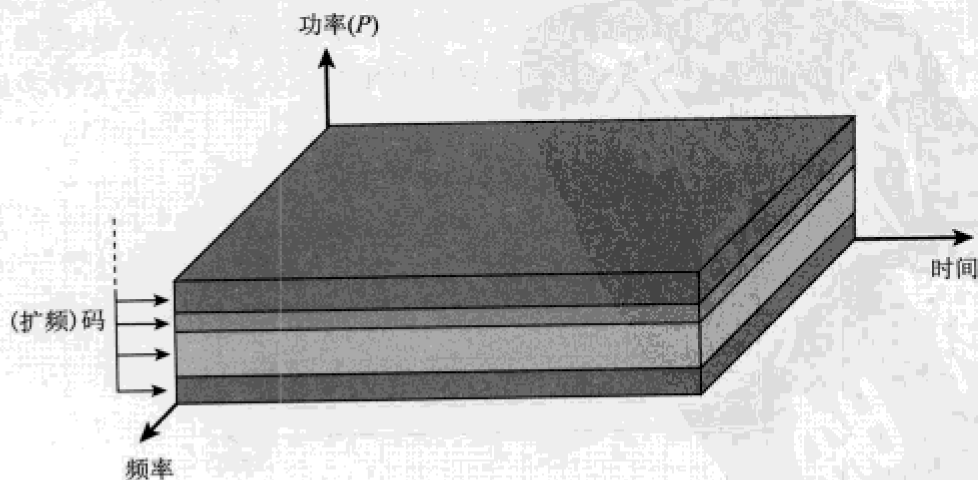


图3.12　CDMA(码分多址)

- 如果源比特速率低,将被充分扩频,所需发送功率较低,如图中薄一点的层所示。
- 如果源比特速率高,扩频不很充分,所需发送功率较高,如图中厚一些的层所示。

在 FDMA 和 TDMA 这类带宽有限的多址接入技术中，主要干扰是大范围频率复用造成的同信道间干扰，而在 CDMA 中，主要干扰是上行用户间干扰。一个基本原因就是上行用户间的干扰随累积功率递增，单小区内同时通信的用户越多，每用户的性能也越差。

根据用于调制的扩频信号的不同，CDMA 可分为以下几类。

- DS-CDMA（直接序列 CDMA）。
- FH-CDMA（跳频 CDMA）。
- TH-CDMA（跳时 CDMA）。
- HM-CDMA（混合调制 CDMA）。
- MC-CDMA（多载波 CDMA）。

在 DS-CDMA 中，当发送端（移动台或基站）数据信号以可取的码片速率和处理增益进行传播时，采用用户指定的伪噪声码进行扩频，接收机用完全相同的扩频码序列恢复出原始信号。结果每个信号因此被扩展到整个无线连接的带宽中。如图 3.13 所示，干扰可以来自各个方向，这一点与窄带蜂窝系统相反。

DS-CDMA 的频率复用因子是 1，也就是说所有用户占用相同的频带来传送信息。DS-CDMA 具有抗多径衰落的固有优点。实际上，像 GSM 这种基于 TDMA 的系统也可以利用跳频技术来对抗多径衰落，这样也等于是实现了扩频。另一方面，由于共享频谱，DS-CDMA 相比于 TDMA 和 FDMA 更容易受到多用户的干扰。

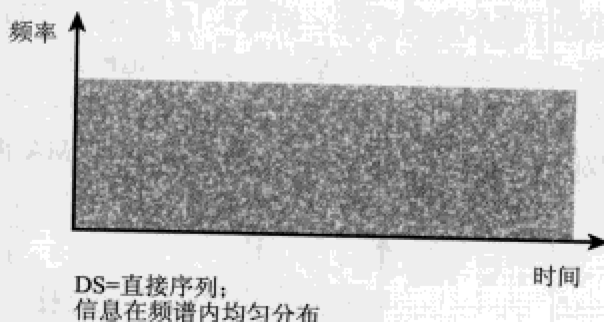


图 3.13 DS-CDMA（直接序列 CDMA）

如图 3.14 中所示，FH-CDMA 通过在发送信号时改变载波频率来扩展带宽。也就是说，在特定的时间间隔中，载波频率保持不变，但随后将根据扩频码跳到另一频率，从而实现信号的扩展。

根据载波信号的跳频频率，FH-CDMA 可以分为两大类：快跳频技术和慢跳频技术。快跳频调制技术中，跳频频率通常高于符号速率，而慢跳频技术中，跳频频率通常低于符号速率。在 FH-CDMA 中，实现像功率控制等 CDMA 的一些基本技术要比在 DS-CDMA 中更为简单。部分是因为该技术用于蜂窝系统时的频分特性。不过，产生高的跳频速率则是 FH-CDMA 中的一个更复杂的问题。

TH-CDMA 技术把传输信号按帧进行划分，这些帧又进一步细分成小的时间间隔。在传输时间内，数据脉冲通过使用码序列在帧之间跳跃。原则上讲，目的是为了选择码序列以尽可能减少同一频率内同时进行的传输个数。这种方法的最重要的思想是综合前述方案的优点，为特定的应用建立一种更方便的技术。这些 CDMA 技术的结合产生了不同的混合技术，如 DS/FH、DS/TH、FH/TH 和 DS/FH/TH。

与 DS-CDMA 不同,MC-CDMA(如图 3.15 所示)在整个频带中同时使用多个而不是单个载波。MC-CDMA 的发送端在所要求的频带内通过扩频码将原始数据扩展到不同频段的子载波上。MC-CDMA 技术主要分为两类。一类是使用给定的扩频码对原始数据扩频,然后调制到不同的子载波上,另一类则与 DS-CDMA 类似。

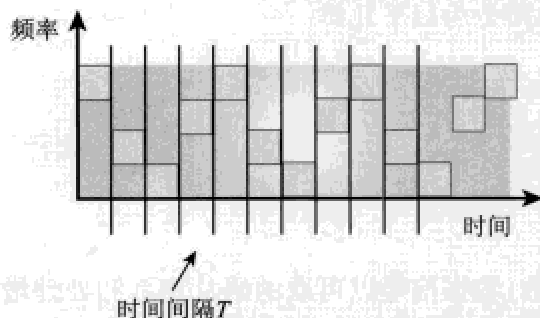


图 3.14 跳频码分多址(FH-CDMA)

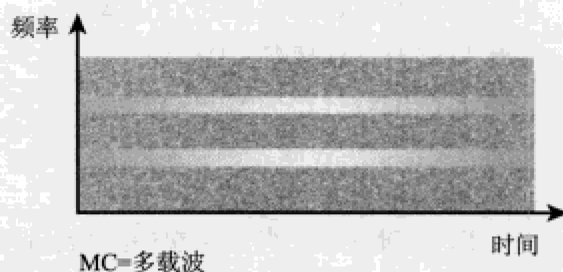


图 3.15 MC-CDMA

除了上述广泛使用的多址接入技术以外,目前,OFDMA(正交频分多址)技术日益引起了通信业的重视。如图 3.16 所示,在 OFDMA 技术中,各活动用户分配有一个或者一组频道。整个共享频带基于频道的正交划分,因此能有效利用频带。分配的频道数可以根据传输数据数量的大小灵活调整。OFDMA 可以结合各种跳频技术,也能吸收时分信道的优点。与跳频结合时,OFDMA 很容易获得扩频方法的主要优点。

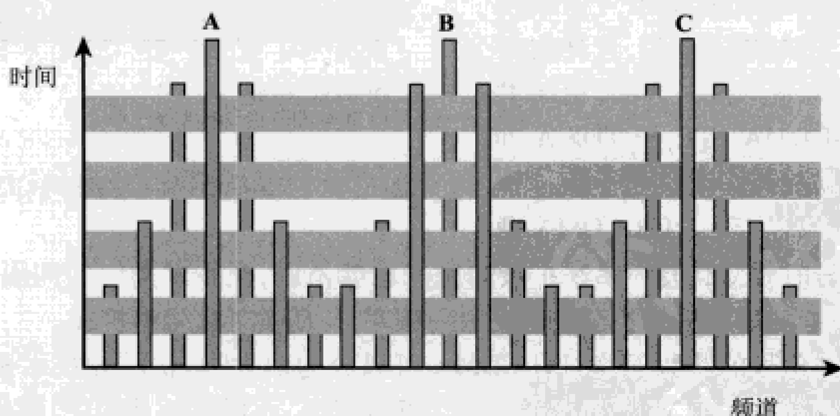


图 3.16 OFDMA

3.4 设备移动性

移动性使终端用户可以在任何地方、任何时刻都能进行通信,但它也对蜂窝网络架构提出了严格的要求。设备在多径信道中移动会引起严重的衰落和多谱勒效应,除此之外,保持移动设备到网络的连接、管理其移动性不仅是任何蜂窝网络都必须具有的功能,同时也是一个巨大的挑战。

一般来说,网络可以通过寻呼、位置更新和切换连接等功能来解决这一问题。切换机制保证移动台从一个基站区域(小区)移动到另外任一基站区域时,无线连接能切换到目标基站而不发生中断。此外,位置更新过程则使网络能跟踪用户在网络覆盖区域中驻留的位置,而寻呼是为了联系到被叫的手机。即使移动台和网络之间没有连续的活动无线连接,位置更新和寻呼机制也能保证网络联系到移动台。对于上述这些功能,需要特别注意降低移动设备功耗的问题。

为了跟踪移动设备,整个地理区域分为LA(位置区),每个位置区是一个逻辑小区群,如图3.17所示。手机开机或位置区改变时会进行位置更新。手机通过来自网络的位置更新请求启动位置更新过程。经过用户信息核实后,网络就会对位置更新请求做出响应,提供新的位置信息并取消旧的信息。位置更新可以周期进行或者按预定的时间进行。

在寻呼中,假设移动设备是被叫方,其当前位置可通过查询归属位置寄存器和访问位置寄存器得知。如果为了某种目的对整个位置区进行寻呼,这种技术叫作同时寻呼。也可以只对LA的一部分进行寻呼,这个部分称作PA(寻呼区)。如果第一次没有呼到被叫方,则顺序在其他寻呼区中进行寻呼,直至完成定位过程,这种方法称做顺序寻呼。

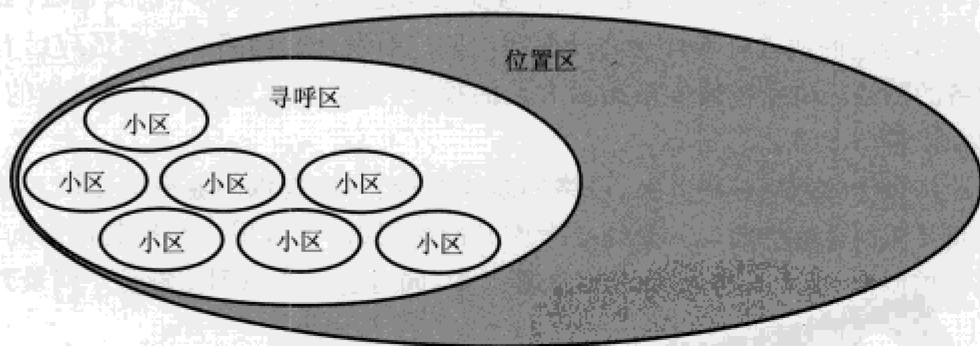


图3.17 小区、寻呼区(PA)和位置区(LA)之间的关系

这种机制虽然简单,但当蜂窝系统中的手机数量增加时就会遇到严重的问题,不仅增加了控制信令开销,也浪费了无线资源。主要原因在于呼入次数和越区次数的增加。此时,如果通过小区分裂来提高系统容量,那么移动性处理就会导致信令开销的增加。为了降低信令开销并优化网络容量,就需要对小区大小及LA和PA进行仔细的设置。在同时寻呼的情况下,假定LA = PA,只要LA改变,所产生的寻呼开销和接入开销之间有相反的作用。换句话说,小的LA对应小的寻呼开销,但接入开销变大,而大的LA会使广播寻呼消息的开销增加,但位置更新的开销降低。

移动性处理的开销能够降到多大程度而不对网络的整体性能带来负面影响,取决于在网络具体所采用的移动性管理体系。在中心结构的分级式移动性管理体系中,信令开销会在高层节点累积,分布式网络体系能使信令开销较为分散,但这不一定能提高移动性管理的效率。

3.5 网络传输

除了无线通信的基本特性和设备移动性造成的制约因素之外，网络传输以及对骨干传输的适配也对网络架构和设计与部署提出了严格的要求。虽然“传送”(transpot)和“传输”(transmission)这两个词有时是通用的，但它们的意思和目的不同。传送是传输使用的功能过程和协议，因此它不一定要和传输过程中的物理连接联系起来。尽管它可能对传输方式产生影响，但在很大程度上，它可以独立地发展。另一方面，“传输方式”则指那些把信号从一点或多点传递出去的行为。从这个方面看，对传输过程的影响可以是间接的或直接的，可以有或没有中间的存储转发。因此传输技术可以按照交换方式区分，如分组交换传输、电路交换传输或光纤传输等传输技术。

矛盾在于，尽管从资本开支和运维开支方面来看，传输结构是网络中成本最高的一部分，也是网络运行的主要瓶颈，但网络架构通常要求在网络部署的初期，传输部分对网络体系是不可见的。结果在网络配置的时候就会遇到困难，而此时更改已为时过晚，这个时候问题就会真正地显现。一个重要原因是，和网络架构中的其他域（如空中接口）相比，传输的演进有其自身的规律和周期。新设计的网络必须要适应已有传输体系设备的制约。更新传输体系需要大量的投资，也需要运营商和其他机构的协调，实现起来很难。

要达到最优的网络解决方案，网络的总体结构、网络提供的业务类型以及传输骨干网之间要做到良好的匹配。必须要考虑到网络层级、传送用户和控制信息的方式、网络的可扩展性、所需业务及 QoS 要求等因素，同时还要考虑到传输骨干网及其升级潜力。

图 3.18 充分地反映了 UMTS 网络（如版本 4 或版本 5）的传输骨干网的起点，它具有一个完全中心控制的网络结构。如图所示，根据所需要的容量、现有骨干网设施、无线接入的覆盖等的不同，传输骨干网媒质及其拓扑结构也显著不同。接入网的物理层拓扑结构可以是树形、星形、链状、环行及其组合，在逻辑上呈现为星形，而在接近核心网的更高层，经常采用逻辑上是网格的环行拓扑。

在 UMTS 网络中，用户平面业务从 B 节点到 CN（核心网）是在不同的层级中处理的。控制业务与用户平面紧密相连。抛开现有分层体系背后的原因不谈，对传输骨干网来说，网络层级越高，聚积的业务量就越大。因此高层网络单元很容易成为网络的瓶颈。因此传输容量必须要与网络层级相匹配，高层级需要光纤这样的大容量传输手段，而在网络边缘，微波传输是更灵活、成本更低的替代传输手段，特别在扩容时。

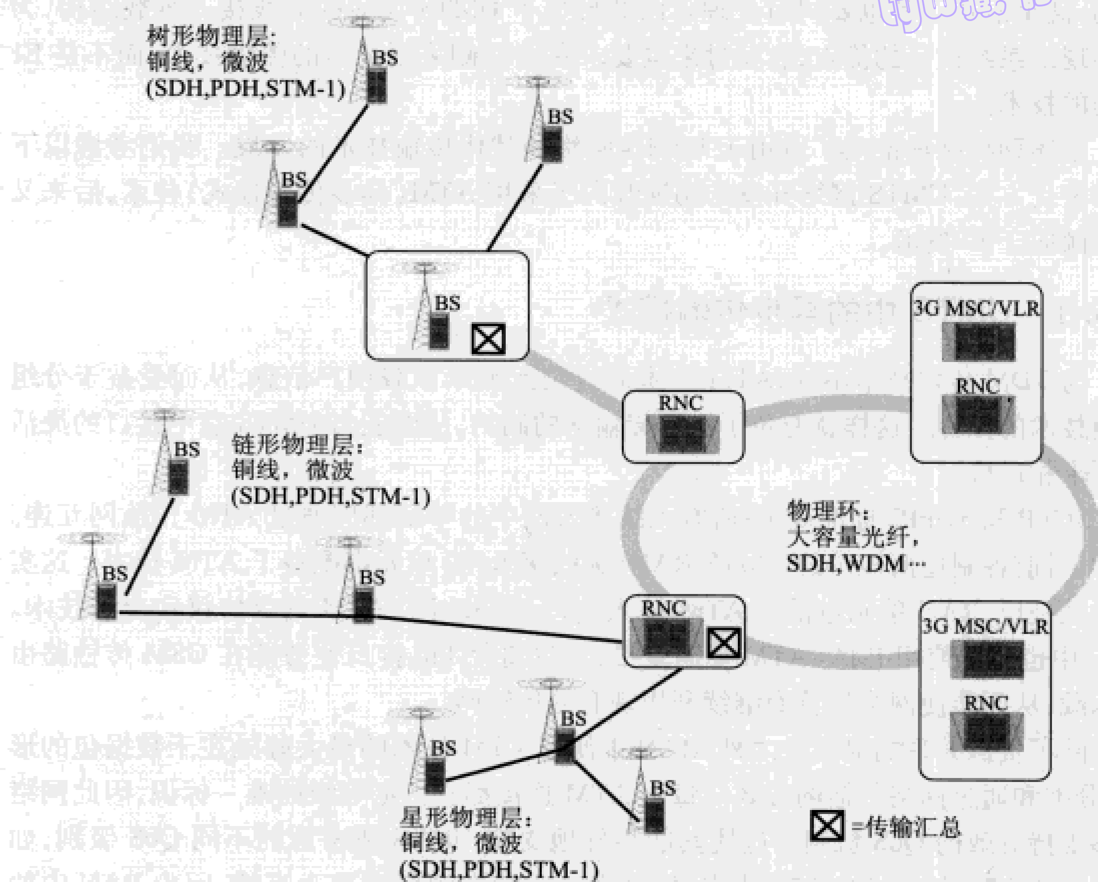


图 3.18 UMTS 骨干传输网示例

3.6 UMTS 中的替代传送技术

蜂窝网骨干网传输目前主要是 TDM(时分复用技术),忽略了当前网络架构从电路为中心到数据为中心的变迁趋势。即使新出现了 PS(分组交换)技术的网元,如 GPRS(通用分组无线业务),它也必须采用已有的传输设施。此外,各种业务都还是在传统的传输技术上进行传送,如 PDH(准同步数字系列)和 SDH(同步数字系列)。随着网络向多媒体和以数据为中心的解决方案发展越来越快,目前的传输已不能满足数据业务的需求。基于 TDM 的传输技术原本是为电路交换业务开发的,不适应数据业务灵活高效的要求。TDM 技术按照时分的方法分配传输资源,在带宽共享问题上对语音和数据业务的处理方式是相同的,没有考虑数据业务中突发业务的固有特点。数据业务的增长要求传输网络能够更灵活高效地处理数据分组流。TDM 对数据和语音业务的同等处理方式、它死板的带宽分配方式不能够支持带宽的细分,带宽分配余出的部分被浪费,而这些带宽本可以用于其他业务。

另一方面,WCDMA(宽带 CDMA)空中接口设计的出发点是假设大多数业务是突

发的，甚至语音业务也要同时处理。因此形成了 UMTS 灵活的无线接入承载结构，为了体现出系统设计的优点，它反过来也要求在网络侧采用灵活的传输技术，而不是 E1 这类的技术。

上述种种制约推动了适用于 UMTS 网络的替代传输技术的发展。我们考虑以下两种替代方案：UMTS 网络开发的初期倾向于采用 ATM（异步传输模式）技术，后来又逐步倾向于 IP 技术。

3.6.1 UMTS 中的异步传输模式

与 TDM 传输技术不同，ATM 技术通过信元流来承载用户信息，从而受益于分组交换技术的原理。这样就避免了已有传输网的制约，从而能与 UMTS 空中接口的灵活性要求相适应。

3GPP 和 3GPP2 标准规定：所有无线接入网中的单元都应通过 ATM 传输网互连。这样，目前各制造商提供的 UMTS RAN（无线接入网）单元都配备了 ATM 技术。这实际上就是说，RAN 单元包括了 ATM 接入端口，并采用了 ATM 信令协议和交换技术。RAN 中也可能使用 IMA（ATM 反向复接）。这将使 Iub 接口业务能在 GSM 传输路由上承载，从而能使网络运营商继续利用现有的传输网。

除了资源共享的灵活性之外，RAN 中使用 ATM 技术的最大好处在于数据包的形成、分类和通过网络传输的方式。每个 ATM 连接都有特定等级的唯一标识，因此网络能够支持有效的 QoS 机制。这使其能很好地支持 UMTS 所考虑的不同 QoS 级别，如同时支持 RT（实时）和 NRT（非实时）业务。也使资源管理更为有效，因为 RAN 中的 RNC（无线网络控制器）能够在网络中对业务负荷进行调度和优化。

尽管 ATM 去除了 TDM 中的种种制约，但产生了新的问题：ATM 信令太复杂，使网络产生了不希望有的延迟和负荷。另外，在规模效应方面 ATM 也拖在后面，而这一点正是 IP 技术的重要优点。因此，从 ATM 过渡到 IP 成为 3GPP 和 R4 及 R5 版本关注的焦点。

在目前的 UMTS 结构中，运营商的传输网络包括基站、节点 B、RNC、基站控制器、移动交换中心、GPPS 服务节点、运维中心。因此，无线接入网中基于 ATM 的业务可以在 E1 用户网络接口 ATM 或 E1 IMA 上传输，或在一个或多个 E1 线路或 STM-1（同步传输模式 1）链路上传输。为了支持不同的业务类型，采用了用于语音和数据的 AAL2（ATM 适配层类型 2）和 AAL5（ATM 适配层类型 5）。传输媒质可以有光纤、E1/T1 铜专用线、微波和数字用户线，视规模效应和可提供的媒质类型而定，也有可能把几种不同的传输媒质组合起来使用。虽然光纤因其速度和容量是最好的传输媒质，但 E1/T1、微波和 DSL 给传输网引入自己的优点，在很多时候，由于成本、基建以及与 2G 和 3G 网络的共存等原因，只能考虑这些传输方式。

虽然 UMTS 网络初期主要是 ATM，3GPP 已开始准备向 IP 传输过渡。ATM 原来的设计思想是在保证语音业务延迟和抖动要求的情况下提供更好的带宽细分性。由

于数据包太小,处理数据包的效率就不高,且不能按不同的业务流进行优化。如果不需要 ATM 的细分性(如链接速率很高并且延迟也不很严重)时,用 IP 就更为高效和有利。但为了保证过渡的连续性,IP 可以叠在现有 ATM 骨干网之上,因此在一定时间内,ATM 仍将在蜂窝网络中起重要作用。

3.6.2 IP 传输

随着全球范围内 IP 协议使用的快速增长以及电信和 IP 业务的平滑会聚,在蜂窝网络中使用 IP 传输已经成为潮流。基于 IP 的传输已经在固网中得到广泛的应用,显示出了 IP 相对于 TDM 或 ATM 网络的健壮性、支持分布式功能结构的能力和网络拓扑的灵活性。IP 传输得益于其规模效应、开放性和简单易用的特性。它不仅能满足 UMTS 网络的要求,也减轻了 ATM 传输技术的制约,起码对数据为中心的业务是这样。

IP 指一系列由 IETF 规定的协议栈,它形成了因特网的支柱。所有业务(如邮件、网页浏览、文件下载、游戏等)都使用 IP 通过全球网络传送数据。每个数据包都由全球唯一的地址标识,因此从源节点到目的节点的数据传输只需要通过简单的寻址和路由机制来处理(图 3.19)。

结合 TCP(传输控制协议)等其他高层的协议栈之后,IP 构成了一种简单灵活的数据传输机制,世界上各种异构网和子网络中的任何两个连接设备中都能藉此传输任意类型的数字信息。若某个 IP 主机(如 PC、移动设备或有全球 IP 地址的任何 IP 设备)欲发送一条信息到目标 IP 设备,这个消息将被封装在 IP 包中。只要提供 IP 包中包含的目标终端设备 IP 地址以及因特网中的 IP 路由器,就可以很容易地把这个包传送到目的地。从原则上来讲,这一过程适用于因特网上的所有业务。

IP 传输的简单性、开放性和灵活性,以及其全球普及程度也是 UMTS 考虑 IP 的重要因素。实际上,随着 GPRS 产品的出现,IP 已经开始进入蜂窝网络。根据 GPRS 使用的现有协议可以向移动终端提供分组数据业务,例如通过分配 IP 地址给这些移动终端。UMTS 分组核心网采用路由与因特网连接,这使其能在一定程度上为移动用户提供 IP 移动性和移动因特网业务。

不过,在现有形式下把移动网络和 IP 进行融合还面临着新的障碍。目前的 IPv4 版本还是 20 世纪 80 年代初制定的,那时还不能预见因特网的普及。IPv4 原本未考虑支持多媒体业务,但 UMTS 网络同时既要支持 CS 业务,也要支持 PS 业务,这样,QoS 支持问题和 IPv4 的其他传统缺点(如地址空间有限)成为移动网络引入 IP 的基本障碍。新版本 IP 的出现(如 IPv6)解决了这两种问题。升级到 IPv6 的分组 CN 可以很好的满足 UMTS 网络的关键要求,可承载 RT 和 NRT 业务。使用单一技术的全 IP 核心网将能使运营商简化网络结构,降低网络复杂性,并能在支持有 QoS 保障的多业务的同时使业务的成本降低。

需要注意的是,从 ATM 到 IP 转变是一个巨大的挑战,因为改换传输网络需要大量的投资。这种过渡最有可能在不同的网络层级以不同的周期出现,最有可能先从传

输网开始，然后是核心网，再扩展到RAN（无线接入网）。因此，实现网络的全IP需要很长的过程。不管过渡周期如何，3GPP R5允许运营商在所有核心网和传输功能中采用IP。

向IP方向发展明显要改变网络结构的演进。可预见的主要改变体现在网络的分级结构上。IP将使网络结构向扁平结构发展。简单地说，传输网络将会显著地推动网络结构的发展。

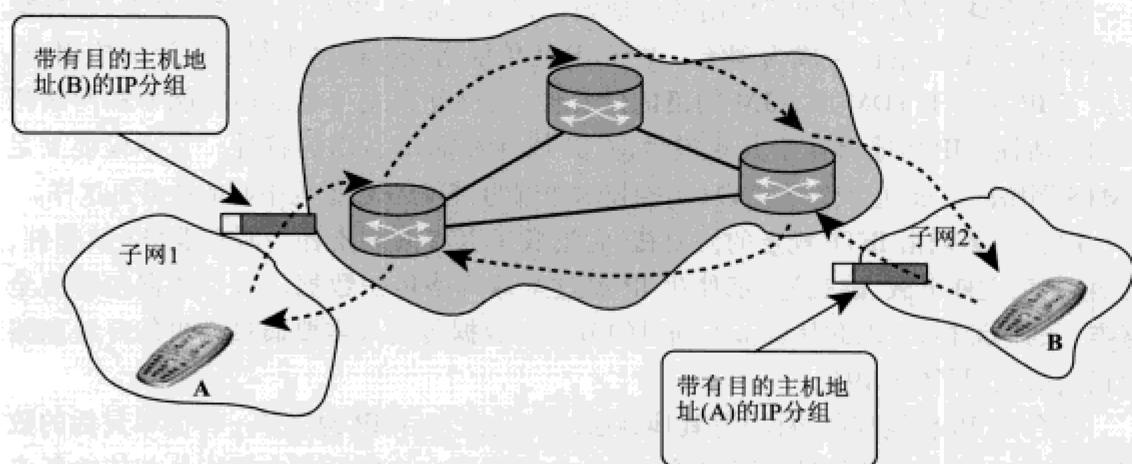


图3.19　IP分组从源传输到目的主机的示意图

3.7　网络管理

网络结构设计中的一个重要问题是如何监控网络的整体运行，并及时排除故障。一般来说，网络管理可以看作是一种业务，该业务利用各种方法、工具、应用程序和设备使网络运营商能够监视和维护整个网络。对于典型的集中式移动网络，网络管理（简称网管）是从某个很可能是远程的特定位置监控整个网络的能力。全球移动网络的高速增长也使网管成为一个关键部分，网络结构设计初期就应予以考虑。网络的基本功能必须能使运营商控制和维护其网络和业务。近年来的发展说明，运营成本实际上已经成为网络运营商资本投入的主体。

在这种情形下，网管应对每个网元、传输方式、交换与存储子系统等设置专用的管理功能，它们一起形成了整个网络管理系统。为了有效地监视网络运行并排出故障，这些管理实体必须能协调工作。此外，网管在网络软件升级、容量和业务管理方面也起着关键作用。还有一个重要作用是根据网络业务行为的随机变化来调整和优化网络运行。

鉴于网管在实际网络中的重要性及其广泛的涉及面，国际标准化组织（ISO）也试图制定相关的框架和范例，用于设计作为网络结构一部分的网管系统。尽管这样，不同厂商提供的网络管理系统可能不同，与其网络单元管理系统的结构有关。

网络管理系统的高级结构

目前的通信网管都是以电信管理网(TMN)为基础的。它给出了管理电信网络的通用模型。TMN 把网络管理自下而上分为这样几层。如图 3.20 所示。

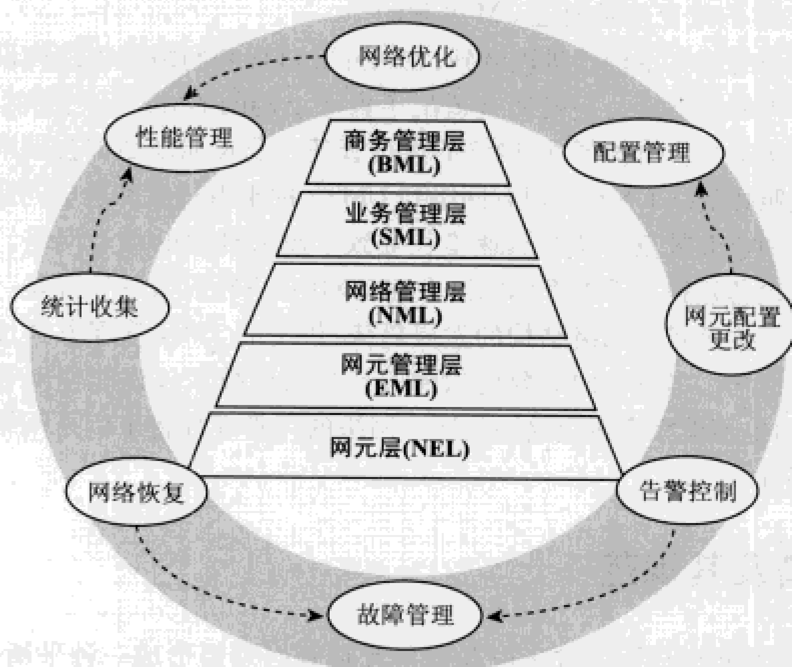


图 3.20 TMN 的金字塔模型以及网络管理系统的一些基本功能

- NEL(网元层):电信网络由不同的物理实体构成,如交换机、控制器、终端等。在 TMN 中,这些都称为 NE(网元),它们形成了 NEL(网元层)。
- EML(网元管理层):该层包括 TMN 中网元和 NML(网络管理层)之间互连所需要的所有功能和资源。
- NML:NML 包含管理网元所需要的所有功能和资源。本文中一般采用三个独立的管理层,即 FM(故障管理)、PM(性能管理)和 CM(配置管理)。
- SML(业务管理层):SML 层的功能包括处理业务和业务提供商之间的互操作,提供到其他企业、客户和供应商的接口,业务级别的协议,统计数据的收集和分析,计费和网络利用率等。
- BML(商务管理层):该高层包括商务目标、商务计划、产品计划、财务问题(如预算)、法律及安全问题。

因此,网管系统不仅应覆盖网元级(如 BTS、RNC 和 CN)的管理需要,也要覆盖网络和业务管理级的管理需要。网元级管理功能包括具体单元的采购安装、故障排除,而网络级功能则是整体的运行维护和网络规划控制。

网络管理系统的主要功能包括 FM、PM 和 CM。

● FM 是网元故障/告警触发、搜集、报送至 NMC(网管中心)的过程。NMC 是执行所有 NML 相关操作的物理点。

● PM 则是从网元搜集统计数值并报送至 NMC 的过程。

● CM 过程是包括添加、删除、修改在内的网元配置工具。例如网管中心对某个小区参数的改变就是通过 CM 处理的。

从网管系统的基本结构不难注意到,它的开发过程和网络总体结构设计是紧密相关的。分级结构的网络不一定能完全适配于扁平结构的 NMS,反之亦然。NMS 还必须要考虑到网络运行及可扩展性,网络的运行管理以及长期规划都会带来网络扩张的问题。还必须照顾到从 GSM 等现有网络到 UMTS 的平滑过渡和适应问题。

移动设备和业务数量的持续迅速增长导致了超大规模的移动网络。对于这样一个有大量无线设备且种类千差万别的巨大移动网络,进行有效的管理是一项复杂而繁重的基本任务。按照目前网络结构的发展趋势,传统的 TMN 管理方式过分依靠集中式的网络管理结构。尽管面向对象的软件等新的软件技术或许能使网管减轻对网络结构的依赖,但也不能完全避免这一问题。网络的可管理性将来仍是网络结构设计中的一个重要部分。

3.8 频谱及其规范

技术、规范和频谱分配的进步以及经济政策等必须要形成一种平衡的协调组合,方能使新的无线系统成功发展。ITU 等频谱规划部门的主要目的是协调无线电频谱在区域内和全球内的使用,为无线频谱的最佳利用制定规则和建议。如今,通信市场的发展与结构对频谱规范的影响比以前任何时候都要敏感,3G 频谱牌照便是一个例子。与频谱规范机构的本意不同,它所出台的频率政策也能形成不平衡的价值链。根据不同的情形,这一点可能会促进或妨碍通信的发展,如图 3.21 所示。

从系统结构的来看,网络中受频谱规则和计划影响最严重的组件是空中接口、发射机和接收机。空中接口应能在规范允许的范围内有效利用频谱。因此,比较不同的无线系统时,频谱效率是一个基本准则。另外,技术发展的周期必须要同 WRC(世界无线通信大会)的频谱分配过程协调一致,尤其对于那些需要新频率才能实施的新技术。

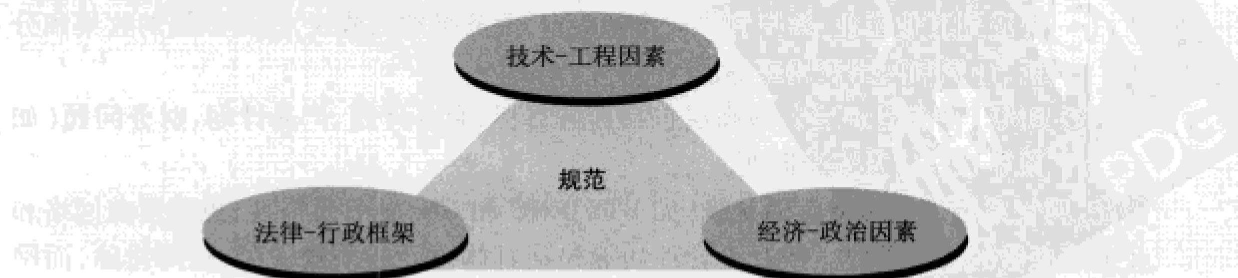


图 3.21 频谱规范过程中不同因素的相互作用

标准的规范化与无线频谱分配和整个通信技术标准是携手进行的。主要推动力来自技术工程和经济政治两个方面。法律人才对整个规范化过程起着重要的作用。

我们已经介绍了无线通信系统有效利用无线频谱的不同技术。所有这些技术的最优结果都不可能超过基本的物理限制,即关于可达到的带宽容量的香农极限。在一定的情况下,增加系统无线信道容量的一种方法就是增加带宽。不过,公众误以为无线频谱是用之不尽的自然资源,但事实上它极其短缺。虽然先进的系统可以通过复杂的编码调制技术、智能天线技术和无线资源管理技术更有效地利用可用的无线频谱,但无线业务需求的高速增长加剧了频谱资源的短缺。因此有必要规范无线频谱的使用,以避免这种稀缺自然资源利用上的低效和混乱。图 3.22 示出了电磁频谱,其中包括 3kHz ~ 300GHz 之间的无线电波频谱。图中还示了这样一点:目前无线应用的频谱分配使用最多的是 100MHz ~ 2000MHz 范围。原因之一在于无线电波的特性:电波频率越高,衰减就越大,覆盖能力越低,功耗越高。

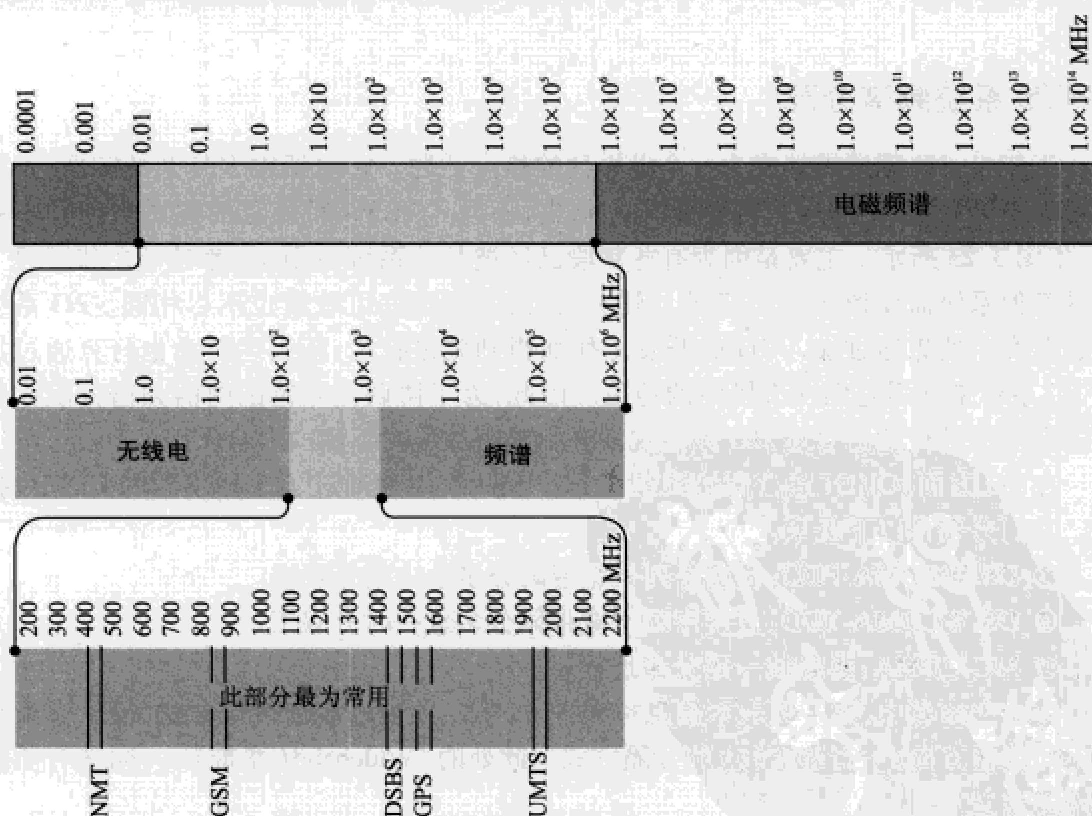


图 3.22 电磁频谱、无线电频谱及其中最常用的部分

因此从技术角度上讲,假设系统的其他技术特性保持不变,那么频率越高,系统实现就越复杂,成本效益也就越低。对于蜂窝系统,高频率应用增加了覆盖范围需要的基站数量,从而增加系统的前期和运营费用。

无线频谱中的政治经济因素更为复杂。一般是由国家的无线电管理部门负责整个无线频谱的规划,很多国际组织也参与其中。基本目标是让珍贵的无线资源既能使

系统提供商和用户满意，又能保证频谱得到最有效的利用。

除了这些因素外，通信市场环境是极度竞争和不断变化的。频谱规划也因此在国际国内都成为了竞争的一个关键要素，于是，频谱的非规范化进程吸引了众多新运营商的加入。此外，国家的利益并不总是协调一致的，因此就有了许多不相同的频谱政策。

无线通信市场急剧增加使未来无线频谱短缺的问题更为严峻。因此有必要在技术方案、无线应用和频谱规划之间建立一个公平合理的契合点。就1G而言，无线频谱是免费使用的（美国是例外，其频谱单元收管理费）。2G也打算继续采用免费的原则，从目前看部分取得了成功。

3G系统的频谱规划给通信系统和商务活动带来了更多的竞争和期望。也使大家认识到，无线频率并不是用之不竭的自然资源。移动用户的数量已经超过十亿，高比特速率业务已经成为移动网络主要提供的内容。随之而来的是无线频谱管理费用显著增加，尤其是在欧洲。3G频谱规划是另一回事，如何评估其影响不在本书范围之内。

UMTS 系统频谱分配

近年来，3G频谱规划成为一个世界性的热点话题。它包括很多复杂的问题，这些问题对不同国家、不同运营商都不同。首先，不同国家3G所规定的频谱空间并不相同，如图3.23所示。主要是因为有些频段已经被其他系统占用，或者对于在邻频段工作的其他系统需要留出保护频带。其次，各国的频谱许可政策也不尽相同。2G系统的运营商自然想通过加入3G的开发工作而得到先进技术，新兴运营商也打算通过加入3G系统来加强它们在市场中的地位。因此，为了协调世界范围内的频谱分配并使各国有效地进行频谱管理，3G频谱规划必须紧密加强国际和国内合作。

在3G方面，OHG（运营商协调组织）于1999年中期通过了3种不同的CDMA技术。它们分别是以下几项。

- DS-WCDMA-FDD：直接序列—宽带码分多址—频分双工。
- DS-WCDMA-TDD：直接序列—宽带码分多址—时分双工。
- MC-CDMA：多载波—码分多址技术。

在这些命名中，第一项表示信息扩频方式，第二项表示多址接入方式，最后一项表示不同传输方向（上行和下行）的分隔方式。此处的“Wideband（宽带）”一词没有任何特殊的含义。

名称中出现宽带这个词起初是因为欧洲和日本的CDMA使用的带宽比美国的要宽。更宽的带宽使系统能引入一些更有吸引力的特性，例如有足够带宽的多媒体业务和宏分集。不过OHG决定这3种CDMA技术使用大致相同的带宽。

WCDMA-FDD下行（从BS到UE）使用的频率为2 110MHz～2 170MHz，上行（从UE到BS）使用的频率为1 920MHz～1 980MHz。空中接口中的两个传输方向由不同的频率分离，双工间隔为190MHz。

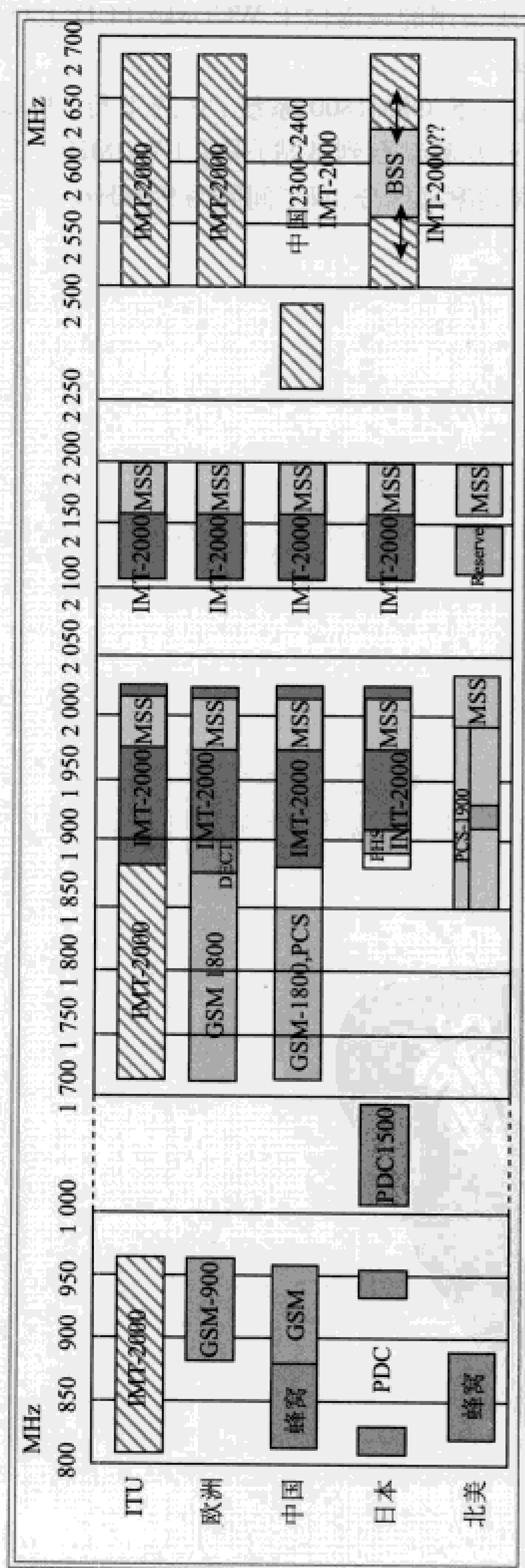

MHz
800 850 900 950 1 000
1 700 1 750 1 800 1 850 1 900 1 950 2 000 2 050 2 100 2 150 2 200 2 250
2 500 2 550 2 600 2 650 2 700
ITU
欧洲
中国
日本
北美
IMT-2000
GSM-900
GSM
蜂窝
PDC
PDC1500
GSM 1800
GSM-1800,PCS
DECT
PHS
PCS 1900
MSS
Reserve
中国2300~2400
IMT-2000
BSS
IMT-2000??

图3.23 3G频谱

TDD方式的WCDMA所使用的频谱位于WCDMA-FDD上行链路的两边，低端带宽为20MHz，高端为15MHz。

为了比较，我们附带提一下GSM1800系统，它的下行（从基站到移动台）采用1 805MHz～1 880MHz，上行（从移动台到基站）采用1 710MHz～1 785MHz。空中接口中的两个传输方向通过不同频率来区分，双工间隔为95MHz。

第 4 章 UMTS 无线接入技术总述

本章简述各种 UMTS(通用移动通信系统)无线接入技术。正如 3GPP(3G 合作伙伴项目)规范所提到的,UMTS 不是单个技术或接入手段,而是精选技术的组合,其趋势是寻找能使这些接入方法共同工作的机制,使得终端用户有足够好的覆盖率,并且有充足的频谱和平台来保证各种业务的功能。

目前,3GPP 规范中认可 3 种主要接入技术。

- WCDMA(宽带码分多址接入)以及在第 3 章中提到的它所选择的版本。就目前 UMTS 而言,FDD(频分双工)版本是这些版本中最有意义的。此外,WCDMA 将被 HSDPA(高速下行分组接入)加强,它能提高下行链路的数据速率。
- GSM/EDGE(全球移动通信系统/增强数据 GSM 演进)无线接入。它是 3GPP R99 发展的基础。
- 补充接入技术。包括 UMTS 系统正在或将要评估的各种候选接入技术。WLAN(无线局域网)自然也在其中,人们正在研究它所能起的作用。

4.1 WCDMA 要素

UMTS 使用的主要无线技术是 ETSI(欧洲电信标准组织)于 1998 年选定的 FDD 和时分双工(TDD)版本的 WCDMA 技术。像传统的 CDMA 一样,扩频技术是 WCDMA 的基本技术,但与之前不同,它采用不同的控制信道和信令、更宽的带宽,以及一系列增强技术来满足 3G 系统的需求。下面简要介绍 WCDMA 无线技术,以便读者理解 3G 空中接口的基本构造和运行情况,并了解网络结构的一般要求。WCDMA 的基本特征,例如软切换、功率控制、码字管理、针对空中接口的业务处理机制等等已经表明,明确地分配在整个网络架构中的各种功能都已就绪。

4.1.1 基本概念

WCDMA 所使用的基本技术是 DSSS(直接序列扩频)技术,其原理如图 4.1 和图 4.4 所示。假定无线信号从 BS(基站)向 MS(移动台)传输。在基站端,速率为 R 的发送信号与一个宽带扩频信号合并,使频谱扩展,产生一个带宽为 W 的扩频信号。在移

动台,接收信号与同一扩频信号相乘。如果移动台本地产生的扩频信号与扩频码/扩频信号同步,相乘的结果就是原始信号再加上一些更高的高频分量,这些分量不是原始信息的组成部分,很容易滤掉。另外,如果移动台处有任何干扰信号的话,扩频信号对它的作用如同 BS 对原始信号的处理,干扰信号将被扩展到扩频信号的带宽。

这一过程使 WCDMA 更健壮、更灵活、更能抵抗干扰,并能抵御人为干扰和侦听。不过,为了实现这个功效,WCDMA 比基本的 CDMA 占用了更宽的带宽。更宽带宽的好处是 WCDMA 可以在无线接口(Uu)中使用多个信道。考虑到一个 WCDMA 空中接口的有效带宽是 3.84MHz,再加上保护带宽,WCDMA 需要的带宽是 5MHz,如图 4.2 所示。

根据计划,WCDMA 的无线部分应能够工作在不同的频段上,如表 4.1 所示。

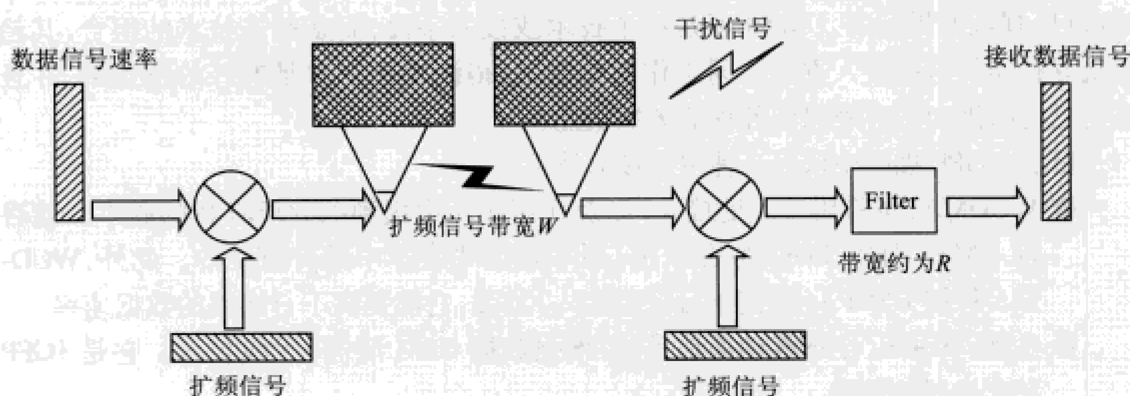


图 4.1　直接序列扩频的基本技术

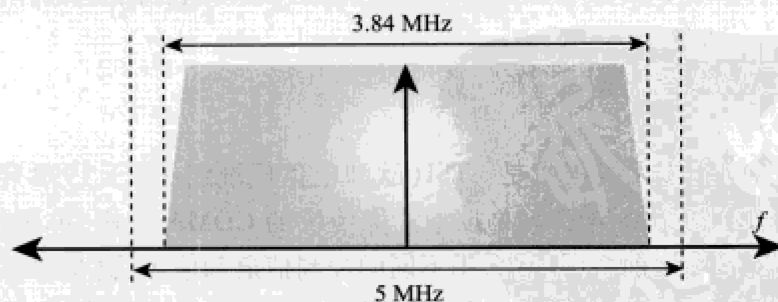


图 4.2　WCDMA 单向载波示意图

表 4.1　3GPP 规划的 FDD 工作频段

工作频段	上行频率(UE 发射,BS 接收)(MHz)	下行频率(UE 接收,BS 发射)(MHz)
WCDMA 核心频段	1 920 ~ 1 980	2 110 ~ 2 170
1 900MHz	1 850 ~ 1 910	1 930 ~ 1 990
1 800MHz	1 710 ~ 1 785	1 805 ~ 1 880
1.7/2.1GHz(美国)	1 710 ~ 1 770	2 110 ~ 2 170
UMTS850	824 ~ 849	869 ~ 894
UMTS800(日本)	830 ~ 840	875 ~ 885

和 DS-CDMA 一样，在 WCDMA 的发射机端，数据信号通过一个用户特定的伪噪声（PN）码进行加扰，使带宽扩展到整个带宽。接收机端用相同的码序列提取接收信号。根据信息论的基本原理，可以得出以下一些简单的结论。

- 欲传输的信息代表一定的功率（如 P_{inf}）。
- 信息传输的带宽越宽，在信息传输带中某一小点上传输信息的功率就越小。换言之，总功率 P_{inf} 就是在整个信息传输带上的积分。
- 欲传输的信息越多，需要的功率就越大。所以，当信息速率不断增加时，P_{inf} 也将不断增长。在这种意义下，欲传输的原始比特速率越高，需要的功率也就越大。

认识到这一点，再结合图 3.12，我们就能看清 WCDMA 是如何处理原始用户数据的每个小单位（称为 1bit）的。

在空中接口中，每一个原始信息比特就像一个恒定体积的“盒子”，但各维的尺寸因具体情况而不同。观察图 4.3 可知，在 WCDMA 中“盒子”的深度（频带）是固定不变的，另外两个维度，功率和扩频因子则是可变的。因此可以得出这样的结论：

- 信号扩展得越好，每比特所需的能量（功率）就越小。这一点适用于原始比特速率低的情形。换言之，扩频因子增加，功率就减少。
- 扩频因子越小，每比特所需的能量（功率）就越大。这一点适用于原始比特速率高的情形。换言之，扩频因子增加，功率减少。

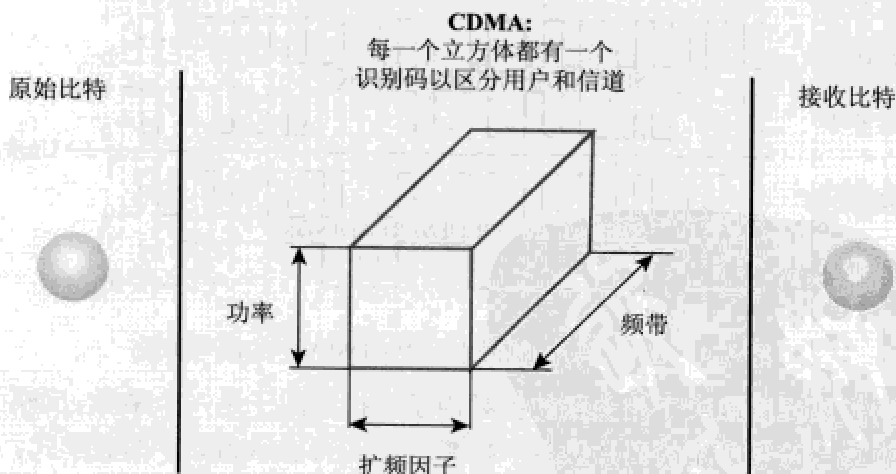


图 4.3 WCDMA 空中接口和比特处理

WCDMA 中一个容易让人混淆的问题是此“比特”并非在所有情况下都是彼“比特”。对于信息，“比特”指原始用户数据流中的信息比特。对于扩频码，这个比特实际上称为码片。根据这样的定义，我们来给出 WCDMA 中涉及的一些基本数据。

用于对原始信号进行扩频的比特速率定为 3.84Mbit/s。这个值在 3G 网络的所有 WCDMA 版本中都是不变的，称为“系统码片速率”（SCR），表示为 3.84Mchip/s。用 SCR 可算出单个码片的持续时间是 1/384 000 = 0.000 000 260 41s。

如前所述，WCDMA 的基本思路是，将原初的数字基带信号乘上另一个更高比特

速率的信号,再通过无线信道传输。这两种信号都由比特构成,必须要分清比特的概念(见图4.4)。因此,有以下几点。

- 在空中接口中,信息以符号的形式发送。符号流是调制的结果。调制之前的用户数据流是经过了信道编码、卷积编码和速率匹配的比特。在图4.3所示,图中央的立方体代表1个符号。根据所用调制方式的不同,1个符号可能代表不同数目的比特。在DS-WCDMA-FDD中,上行链路传输的1个符号代表1bit,下行链路传输的1个符号代表2bit。差别在于上行和下行使用的调制方式不同。
- 用于信号相乘的码字信号中的1bit称为1个*码片*。

那么,接收端如何捕获出想要的信号呢?其原理非常简明:每个接收机使用其特征码提取出想要的信号。将接收的信号和接收机的特定码相乘,得到想要的数据。如果与期望信号相乘的码是正确的,积分后的数据将会呈现出清晰的信号峰值,否则积分后的数据就不会出现这样的峰值供后续处理使用。

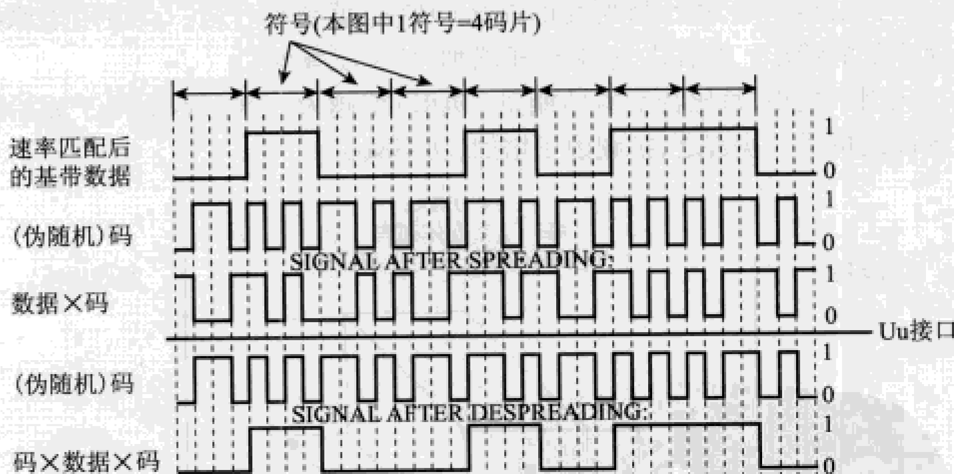


图4.4　比特、码片、符号以及WCDMA中的信号扩频

信号的扩展程度取决于相关联的扩频因子。扩频因子是一个乘数,反映WCDMA无线链路中每一符号所用的码片数量。扩频因子K可表示为如下的数学式:

$$K = 2^k \quad k = 0,1,2,\cdots,8。$$

例如,若$k=6$,则扩频因子K为64,表示WCDMA无线链路上行方向上,1个符号要占用64个码片(参考表4.2和表4.3)。扩频因子也称为*处理增益*(G_p),可表示为所用带宽的函数:

$$G_p = \frac{B_{Uu}}{B_{Bearer}} = \frac{系统码片速率}{承载比特速率} = 扩频因子$$

式中,B_{Uu}代表U_u接口的带宽,B_{Bearer}表示速率匹配后的基带数据的带宽。就是说,B_{Bearer}还包括其他额外的信息,如信道编码和查错保护信息。根据上式,结合考虑上下行每符号所携带的比特数,就可以计算出在WCDMA中可用的承载比特速率。

表 4.2 上行链路中扩频因子、符号速率、比特速率的关系

扩频因子	符号速率(ksymbol/s)	信道比特速率(kbit/s)
256	15	15
128	30	30
64	60	60
32	120	120
16	240	240
8	480	480
4	960	960

表 4.3 下行链路中扩频因子、符号速率、比特速率的关系

扩频因子	符号速率(ksymbol/s)	信道比特速率(kbit/s)
512	7.5	15
256	15	30
128	30	60
64	60	120
32	120	240
16	240	480
8	480	960
4	960	1 920

上述数字只是示意性的，因为用户数据的份额（净荷）与所用的无线信道配置有关。

WCDMA 系统使用了多种不同的码。理论上只要用一种码就够了，但在实际当中，鉴于无线链路的物理特性，WCDMA 系统使用不同的码于不同的用途。不同的码在正交性和自相关特性方面有差异，使它们分别适合于不同的情形。主要有 3 种可用的码，它们是信道码、扰码和扩频码。它们的用途如表 4.4 所示。

表 4.4 WCDMA 中码的类型

	上 行	下 行
扰码	区分用户	区分小区
信道码	区分同一终端的数据和控制信道	区分同一小区中的不同用户
扩频码	信道码×扰码	信道码×扰码

WCDMA 中另一个容易让人困惑的问题就是同一概念可能有多种叫法。这种问题对不同的码也同样存在。例如，根据所使用码的类型，扰码有时会有不同的名字，如称为“Gold 码”（一般出现在与无线链路直接相关的技术文献中）或“长码”。其中“扰码”是最常用的名称。在下行链路，扰码用于区分小区/扇区。在上行链路，扰码用于区分用户（指用户的手机）。

进一步地讲，由于每个用户的数据流都占用了整个频率带宽，必须要以最小的失真检测出正确的信号。使用扩频码就是为了区分在这个频带上的不同传输。扩频码对每个传输是唯一的，它在通信开始时由网络分配。一个扩频码可以看成一把移动台

和网络所用的"钥匙"。双方用这把"钥匙"来打开具有噪声特性的宽带传输信号。或者确切地说,是从有许多无线网络连接的频带中提取出正确的宽带传输信息。

从扩频码的角度来看,小区容量取决于分配给小区的下行扰码的数量(最小为1)。每一下行扰码有一组信道码,每一个呼叫/传输的进行需要一个信道码。实际中,一个扩频码就是扰码×信道化码。如果不使用信道码,扩频码就是扰码。扩频码也取决于所传输的信息类型。从小区向所在区域内各个终端发出公共信息时,要从信道码集合中占去一些信道码。

4.1.2 WCDMA 无线信道

WCDMA 无线接入分配给用户的带宽,以及相关的控制功能是以"信道"的名义处理的。WCDMA 所实现的功能中定义了需要的信道类型及其组织方式。如图 4.5 所示,WCDMA 中的信道组织方式有三层,分别是逻辑信道、传输信道和物理信道。其中,逻辑信道反映发送信息的类型,传输信息反映逻辑信道是如何传输的,而物理信道则是"传输介质",提供了信息真正传输的无线传输平台。

回顾第1章所阐述的系统结构,其信道结构和用途与 GSM 有着显著的差别。"物理信道"表示 Uu 接口上为了不同的目的所实现的不同带宽分配。换言之,物理信道在 UE 域和接入域之间形成了 Uu 接口的物理存在。在 GSM 中,物理信道和它们的结构由 BSC(基站控制器)来识别,但是在 WCDMA 中,物理信道确实存在于 Uu 接口处,RNC(无线网络控制器)不一定知道它们的结构。

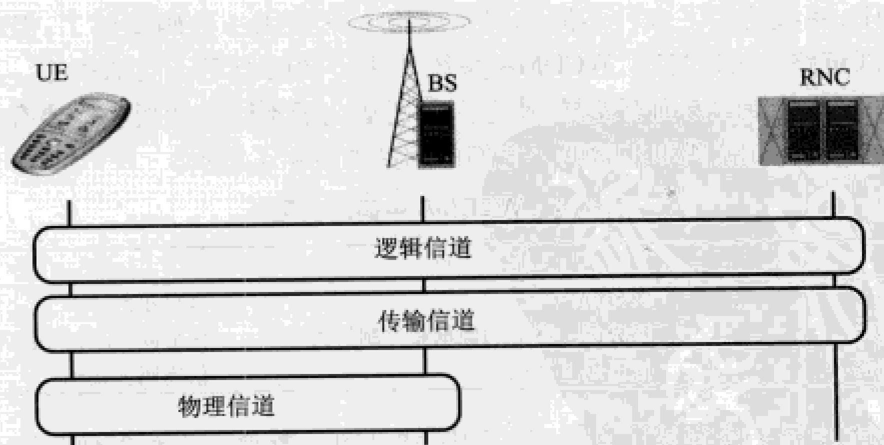


图 4.5 WCDMA UTRAN 中的逻辑信道、传输信道和物理信道

RNC 能"看见"是传输信道,而不是物理信道。传输信道在 Uu 接口上装载不同的信息流,把这些信息流匹配给物理信道的物理部件就是 BS。逻辑信道不是真实的信道,它们可以理解为在不同时刻网络和移动终端应该执行的不同任务。然后这些半实时性的结构体匹配到传输信道上,从而在 UE 域和接入域之间进行实际的信息传输。

对于逻辑信道来说，UE 和网络有不同的任务要执行。因此在每个方向上，逻辑信道、传输信道和物理信道结构都有所不同。简要来说，网络要完成以下任务。

- 它必须通知 UE 关于无线环境的信息，例如本小区和相邻小区中的码值、允许的功率电平等。网络通过逻辑信道向 UE 提供的信息叫做 BCCH（广播控制信道）。
- 当有通信要求到达某个 UE 时（比如移动终端被叫），必须寻呼 UE 以找出它的确切位置。这种网络请求是通过称为 PCCH（寻呼控制信道）的逻辑信道发送的。
- 网络要执行某个可能针对小区中所有 UE 的任务。为此，网络需要用到名为 CCCH（公共控制信道）的逻辑信道。考虑到可能有很多 UE 同时使用 CCCH，所以 UE 必须使用 U-RNTI（UTRAN Radio Network Temporary Identity，UTRAN 无线网络临时识别器）来进行身份识别。通过检查接收到的 U-RNTI，UTRAN 能够将接收的消息正确转接到提供服务的 RNC。有关 U-RNTI 的内容将在第 5 章中讨论。
- 对于专用的活动连接，网络将有关该连接的控制信息通过名为 DCCH（专用控制信道）的逻辑信道进行发送。
- 专用业务：在下行链路方向上，为某个用户服务的专用用户业务是通过名为 DTCH（专用业务信道）的逻辑信道进行传送的。
- CTCH（Common Traffic Channel，公共业务信道）是单向传输信道，仅存在于下行链路方向，用于向小区中的全体 UE 或者某一组 UE 发送信息。

图 4.6 示出了 WCDMA 信道安排的概况。图中的传输信道中，除了一个之外，其余都是必须的。必须的传输信道包括 BCH（广播信息）、PCH（寻呼信道）、FACH（前向接入信道）和 DCH（专用信道）。除此以外，运营商还可以使用 DSCH（下行共享信道）和（HS-DSCH）高速 DSCH 来配置 UTRA。在这些传输信道中，只有 DCH 是专用信道，其他都是公用信道。此处“专用”的意思是说 UTRAN 已将信道分配给它和特定终端之间使用，“公共”的意思是指多个终端可以同时使用信道。

BCH 携带 BCCH 的内容（需要在小区内发送的 UTRA 特定信息）。此信息包括随机接入码、接入时隙、相邻小区等信息。为了能在网络注册，UE 必须能够解码 BCH。BCH 的发送功率相对较高，以便预定的小区覆盖区域内的每个终端都能够“听见”它。PCH 携带寻呼信息，用于网络发起和某个 UE 的连接。FACH 对小区内已知的 UE 发送控制信息。例如，当 RNC 接到来自移动终端的随机接入消息后，响应就是通过 FACH 发送的。此外，FACH 还可以携带下行分组业务。一个小区可有多个 FACH，其中之一必须要配置为低比特速率，以使小区内停留的所有终端都能接收到。DCH 携带专用业务和控制信息（即 DCCH 和 DTCH）。需要注意的是，一个 DCH 可以根据情况携带多个 DTCH。例如，某个用户可以同时有一个语音呼叫和视频呼叫。语音呼叫占用一个逻辑 DTCH，视频呼叫则请求另一个逻辑 DTCH，但它们均使用同一个 DCH。从 UTRA 容量的角度来说，由于专用信道要占用无线资源，因此应尽量使用公共业务信道。人们越来越关注可选的 DSCH。它携带分组业务的专用用户信息（即 DTCH 和

DCCH)，并且多个用户可以共享。从这一方面看，它要比 DCH 好，因为它节省了下行方向上与分组传输相关的网络资源。另外，相对于 DCH，DSCH 和 HS-DSCH 可以快速改变最大比特速率。普遍认为，能偶尔产生突发分组的业务（如上网）将会普及，这使得人们对 DSCH，特别是 HS-DSCH 的关注日益提高。

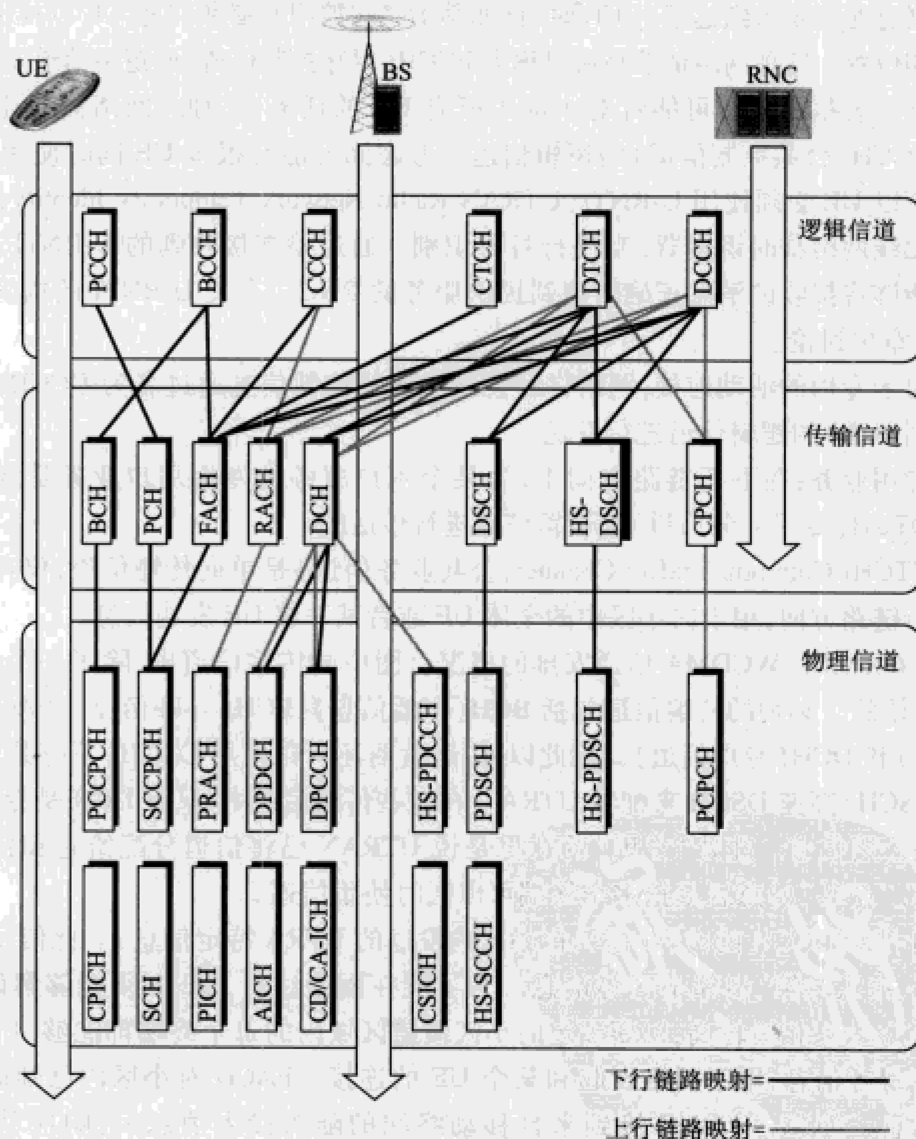


图 4.6　UTRAN 中的信道类型、与相关网络元素的位置关系以及它们在下上行链路的映射

为了增强 WCDMA 系统的数据能力，3GPP R5 制定了一些新的传输信道和物理信道：HS-DSCH 是一个可以由多个移动设备共享的传输信道。与其关联的信道包括一个下行链路 DPCH（专用物理信道），一个或多个 HS-SCCH（共享控制信道），以及用于传输反馈信息的 HS-DPCCH（上行链路专用控制信道），其中 HS-SCCH 也是一个新的信

道。HS-DSCH 信道可以向整个小区发送，也可以通过波束成形天线等方法仅向小区的一部分发送。HS-SCCH 具有固定的速率（60kbit/s，*SF* = 128），用来处理 HS-DSCH 所需要的下行信令。物理层使用具有固定扩频因子（*SF* = 16）的高速物理 HS-PDSCH（下行链路共享信道）来承载 HS-DSCH。若移动设备支持在同一 HS-PDSCH 子帧中使用多码，比特速率能得到大幅度的提高。

上行方向需要的逻辑信道要少一些，只有三种：CCCH、DTCH 和 DCCH。这些缩写词的含义和下行相同。

上行方向有 3 个必须的传输信道：RACH（随机接入信道）、DCH（专用信道）和 CPCH（公共分组信道）。RACH 携带从 UE 到 UTRAN 的控制信息（比如连接建立请求）。另外，RACH 也可以携带少量的分组数据。DCH 与下行一样（即它是一个用于承载 DCCH 和 DTCH 信息的专用传输信道）。CPCH 是为分组数据传输设立的公共传输信道，它是 RACH 的一种扩展，对应下行的 FACH。

信息由逻辑信道收集，并由传输信道组织为预传输格式。然后根据物理信道安排传输信道，再进行传输。其他物理信道则用于无线物理媒介的控制、修正和接入。

物理信道在终端和基站之间，如图 4.7 所示。按照本书开头就提到的网络结构，物理接入（即物理信道）方式和其他层是分离的。理论上，这种安排可以使物理的无线接入介质处在其他层之下。实际应用中，无线接入介质的变化将影响上层，这种方式能使影响最小。

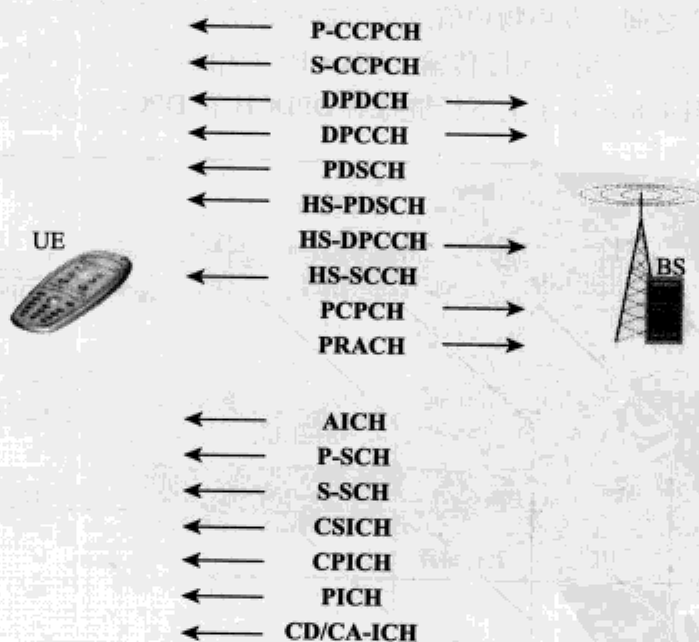


图 4.7　WCDMA 物理信道

P-CCPCH（主公共控制物理信道）携带下行 BCH。小区覆盖范围内的所有终端都能够解调 P-CCPCH 的内容。这一点使 P-CCPCH 的某些特征和其他物理信道相比，就

是一种限制。P-CCPCH使用固定的信道码,其扩频码也因此是固定的。这是必须的,否则终端就不能"看见"并解调出P-CCPCH。P-CCPCH比特速率是30kbit/s,扩频因子为256。由于此信道功率相对较高,因此比特速率必须低,否则干扰就会变大,从而会限制系统容量。因而在这种特殊情况下,扩频码、传输功率和比特速率之间的关系与先前讨论WCDMA基本原理时不同,因为对于该信道定义的这个速率来说,本可以采用更低的功率。

S-CCPCH(Secondary Common Control Physical Channel,辅助公共控制物理信道)携带了两个传输信道:PCH(Paging Channel,寻呼信道)和FACH(Forward Access Channel,前向接入信道)。这些传输信道可以使用相同的或者不同的S-CCPCH,因此每个小区总会有至少一个S-CCPCH。出于和P-CCPCH相同的原因,S-CCPCH的比特速率也是固定的,且相对较低。在后期的版本中,可以通过改变系统设置来提高S-CCPCH的比特速率。S-CCPCH配置方式是可变的:可以根据具体情况对S-CCPCH进行不同的配置,以优化系统性能。例如,可以选择包含或不包含导频符号。在S-CCPCH的各种不同配置中,一种能增加系统性能的配置方式是将PCH信息和FACH复用到S-CCPCH,把PCH相关的寻呼指示复用到另一个单独的物理信道,即寻呼指示器信道(Paging Indicator Channel,PICH)中。

DPDCH(Dedicated Physical Data Channel,专用物理数据信道)承载专用用户业务。DPDCH的大小可变,可以装载多个呼叫/连接。顾名思义,DPDCH是专用信道,用在网络和某一个用户之间。专用物理信道总以成对的方式分配给每个连接:一个信道用于传送控制信息,另一个用于实际传输。DPCCH(专用物理公共信道)在专用连接期间传输控制信息。图4.8示出了上下行链路对DPDCH和DPCCH的处理。

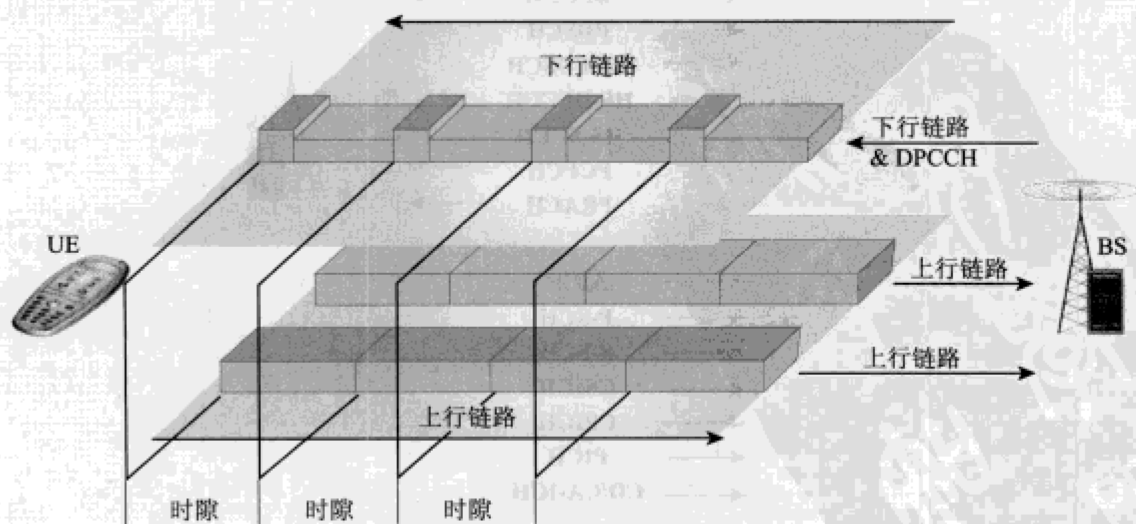


图4.8 上行及下行链路上的DPDCH和DPCCH

下行链路上的DPDCH和DPCCH是时分复用的,DPDCH携带用户数据,DPCCH携带如功率控制数据速率之类的信息。如果DPDCH无信息可传,发送信号就会成为

脉冲形式,这种脉冲存在电磁兼容问题,不过对下行链路没有影响。上行链路的 DPDCH 和 DPCCH 由 I/O 调制区分。即便 DPDCH 没有数据,也不存在脉冲干扰。UE 中 I/O 调制的结果实际上是一个信道,两个信息分支(见图 4.8),这两个信息分支共用一个码资源。

DPCCH 和 DPDCH 一起装载传输信道 DCH 的内容。当这个专用连接出现高峰值比特速率时,系统就会遇到小区内信道码短缺的问题。此时有两种选择:要么增加新的扰码,要么使用公共信道来传输专用数据。不推荐使用添加扰码的方式,它会失去正交性。而使用公用信道资源来传输分组数据一般认为是提高容量的更好途径。下行 DCH 可以提供相应信息,以指示接收 UE 是否需要对 PDSCH(物理下行链路共享信道)进行解码,以得到增加的用户数据。PDSCH 装载 DSCH 传输信道,如前所述,DSCH 对运营商来说是配置时的可选项。

当上行链路需要传输分组数据,而 RACH 的分组传输容量又不够时,UE 可以使用上行 CPCH。相应的物理信道是上行链路 PCPCH(物理公共分组信道)。CPCH 对应下行的 DPCCH。PRACH(分组随机接入信道)携带有关 RAP(随机接入进程,见图 4.9)的信息。终端通过此进程接入到网络中,并能传输少量数据。RAP 有以下几个状态。

(1)UE 解出 P-CCPCH 上的 BCH 信息,得到扰码和可用的 RACH 时隙。

(2)UE 随机选用一个 RACH 时隙。

(3)UE 根据接收到的下行功率电平设置其初始功率电平,向网络发送"前置码"。

(4)终端解出 AICH(Acquisition Indication Channel),以检查网络是否收到了所发送的前置码。如果没有,UE 再以更高的比特功率重新发送。

(5)当 AICH 指示网络已收到了前置码时,UE 在 PRACH 发送 RACH 信息。所发送的 RACH 信息长度是一个或者两个 WCDMA 帧,需要 10ms 或 20ms 的时间。

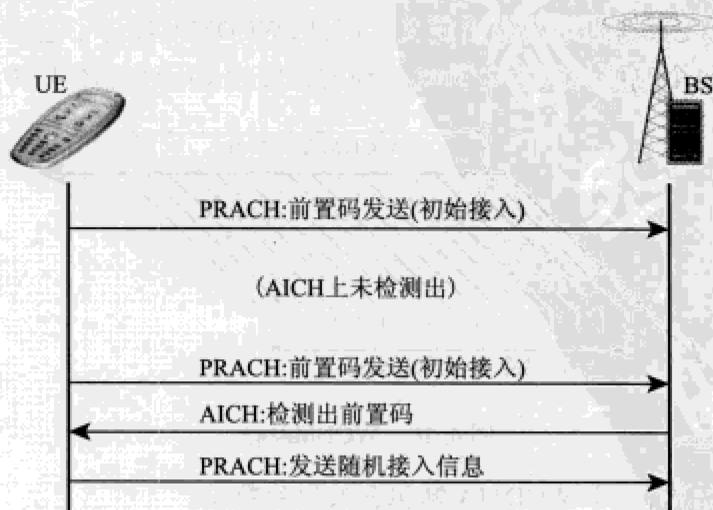


图 4.9 随机接入基本过程

同步信道(SCH)为小区覆盖区域内的UE提供小区搜索信息。SCH实际包含两个信道,P-SCH(Primary Synchronisation Channel,主同步信道)和S-SCH(Secondary Synchronisation Channel,辅助同步信道)。P-SCH在系统的所有小区中都固定使用一个长度为256的信道码。UE检测出P-SCH时,它已经建立了系统的帧和时隙同步,并知道将要接入的小区属于哪个扰码组。

CPICH(Common Pilot Channel,公共导频信道)是未调制的码道,它采用指定给该小区的扰码进行加扰。CPICH专门用于终端进行信道估计,并作为相关公共信道的信道估计参考。导频信号的这种功能类似于GSM突发中间的训练序列。一个小区一般只有一个CPICH,但有时也可以有两个。此时这些信道称为"主CPICH"和"辅CPICH。"小区使用辅助CPICH的例子比如用窄波束天线为特定的"热点"区域提供服务。此时,特定区域使用辅CPICH和主CPICH来为整个小区覆盖区域提供导频。终端连续侦听导频信号,系统的某些关键目的正需要这样,例如切换测量和小区负载平衡。从系统的角度来看,调节CPICH的功率电平便能平衡小区间的负载。UE总是在搜寻导频最强的小区,降低CPICH信号强度将降低小区的吸引力。

列于图4.9中的其他物理信道还包括:CSICH(CPCH Status Indication Channel,CPCH状态识别信道)、CD-ICH(CPCH Collision Detection Indicator Channel,CPCH冲突监测指示信道)和CA-ICH(CPCH Channel Assignment Indicator Channel,CPCH信道分配指示信道)。CSICH使用AICH的空闲空间,用于向UE指示CPCH的存在及其配置。为了避免碰撞(多个UE用同一识别模式),启用了CD-ICH和CA-ICH,用来向UE传输碰撞检测信息。

4.1.3 WCDMA帧结构

为了使无线接入能处理网络和移动台之间的控制操作,如定时、同步控制、传输安全等,必须要对突发数据的结构做出定义。因此,WCDMA包含了这样一个帧结构,它分为15个时隙,每个时隙长度为2/3ms,1帧的长度为10ms(见图4.10)。

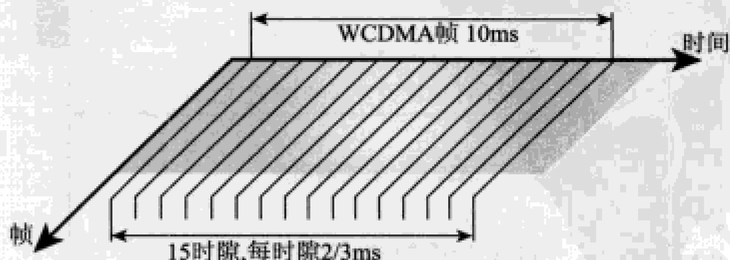


图4.10 WCDMA帧

根据这个帧结构,一个WCDMA帧包含的码片数是:

$$\frac{0.010\text{s}}{0.000\,000\,260\,41\text{s}} \approx 38\,400 \text{ 码片}$$

WCDMA 帧中每个时隙包含的码片数是：

$$\frac{38\ 400\ 码片}{15\ 时隙}=2\ 560\ 码片$$

WCDMA 没有 GSM 中的超帧、超高帧或复帧结构，而是将 WCDMA 帧用系统帧序号(System Frame Number, SFC)编号。SFN 用于 UTRAN 的内部同步和 BCCH 信息传输的定时。

图 4.11 和图 4.12 分别表示上行和下行链路专用信道帧结构。如图所示，专用物理信道在上行链路和下行链路具有不同的结构。

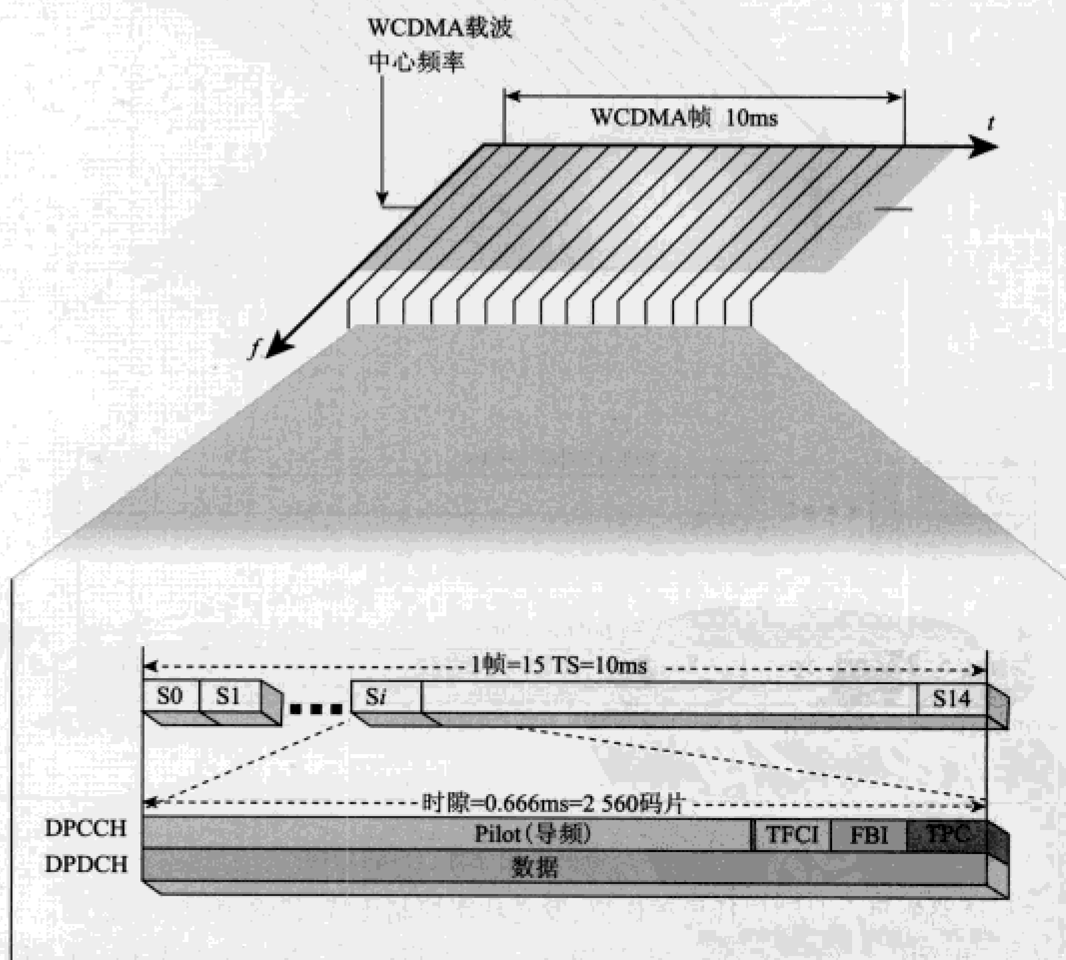


图 4.11　上行链路专用物理信道帧结构

上行链路专用物理信道的帧结构基本依照下行帧结构，差别在于上行链路专用信道 DPDCH 和 DPCCH 不能采用时分复用的方式，因此上行链路专用物理信道采用多码方式实现。需要指出的是，使用多码时，多个并行 DPDCH 使用不同的信道码来传输，但每次连接只有一个 DPCCH。

上行 DPCCH 包括导频比特以支持相干检测所需要的信道估计，TPC(发送功率控

制）发布调节发送功率的指令，FBI（反馈信息）和可选的TFCI（传输格式组合指示）向接收机提供一些瞬时参数，这些参数涉及复用在上行DPDCH中的不同传输信道，与同一帧中传输的数据对应。

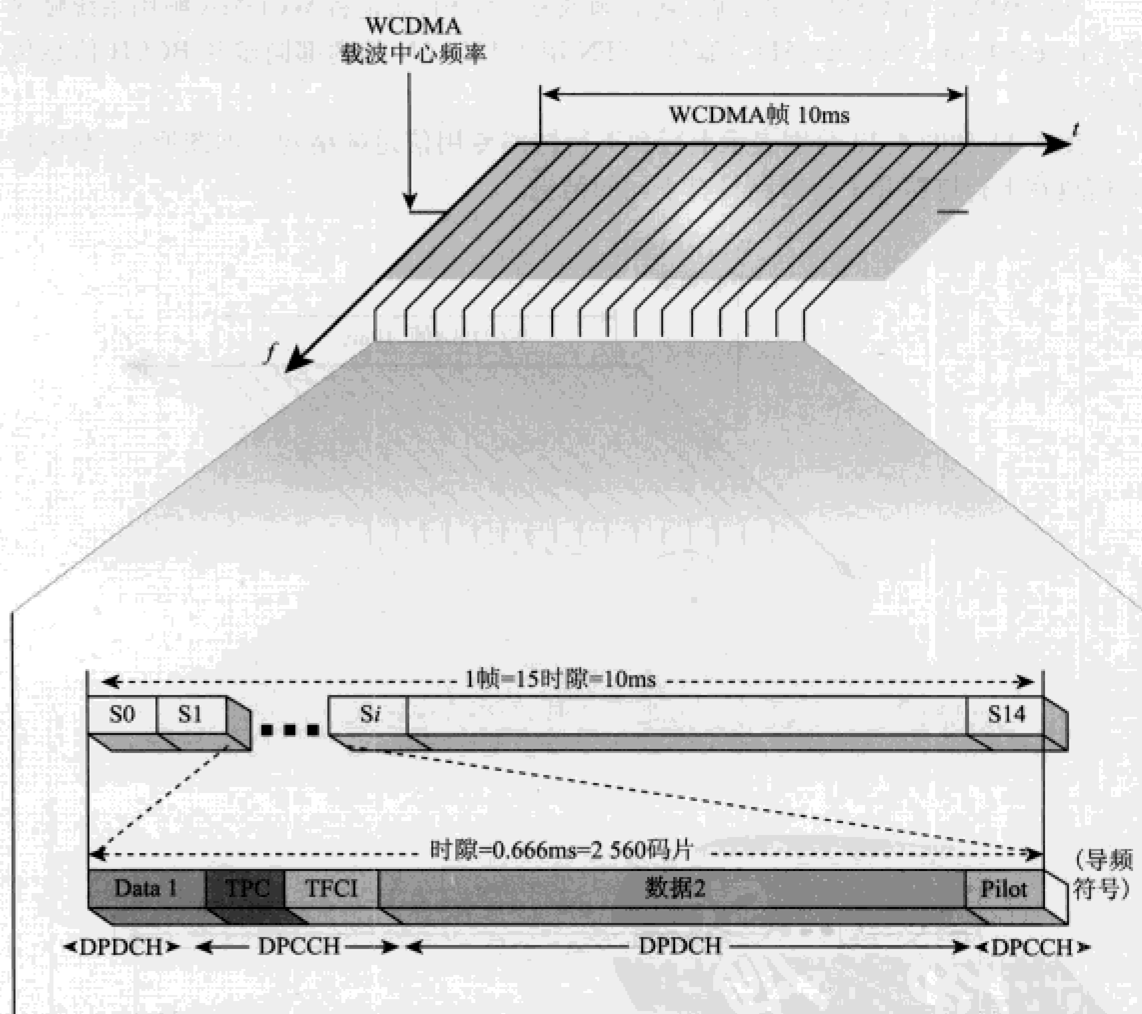


图4.12 下行链路专用物理信道帧结构

下行链路的每个时隙包括导频比特、发送功率控制比特、传输帧指示和数据。

需要指出的是，在一个下行DPCH中，第2层或更高层产生的专用数据（即DCH）以时分复用的方式和第1层产生的控制信息（导频比特、TPC指令和可选的TFCI）一起传输。因此，下行DPCH可视为下行DPDCH和下行DPCCH的时分复用。除了标准化过程中的协调折中这个因素外，这样做的原因如下。

- 最小化移动手机的连续发送。
- 更有效地使用下行链路的正交码。
- 通过上下行时隙偏移最小化功率控制时延。

公用信道的结构和专用信道一样，主要区别是公用信道中没有TPC比特。

最后，表 4.5 总结了前述 WCDMA-FDD 技术的主要特征。这些技术参数使 WCD-MA-FDD 能够达到 3G 移动系统的要求。

表 4.5 WCDMA-FDD 主要技术特征

参　数	标　准
多址	FDD:DS-CDMA
双工方式	FDD
码片速率(Mchip/s)	3.84
帧长(ms)	10
信道编码	卷积码($R=1/2$、$1/3$、$1/4$，$K=9$)；turbo 码($R=1/2$、$1/3$、$1/4$，$K=4$)
交织	帧间/帧内
数据调制	FDD：下行为 QPSK、16QAM，支持 HARQ(HSDPA)；上行为双信道 QPSK
扩频调制	FDD：上行为 BPSK，下行为 QPSK
功率控制	闭环(内环、外环)，开环。步长：1~3dB(上行)；功控周期：1 500/s
分集	在基站和移动台都采用 RAKE；天线分集；发送分集
BS 间同步	FDD：不需要精确的同步技术
解调	MS 和 BS：上行采用基于导频符号的相干解调，下行用 CPICH 进行信道估计
多用户检测	支持，但在第一阶段不采用
业务复用	每个连接支持变速率混合业务
多速率概念	通过可变扩频因子和多码技术支持
切换技术	支持同频软切换及更软切换，支持系统间和频率间切换技术

4.2 WCDMA 增强版——HSDPA

4.2.1 引言

在 UMTS 发展的早期阶段，人们认为数据业务的发展趋势应能遵循固网的经历，共享 IP 业务将成为主流。3GPP 已经提出了“全 IP”的概念，通过创建新的结构模块，例如 IMS(IP 多媒体子系统)，在 UMTS CN(核心网)实现 IP 业务的处理。为了提高网络的整体数据能力，显然应该更关注 UTRAN，特别是其空中接口技术的演进。另一方面 UTRAN 的数据增强版及其空中接口也已经在 R4 版本中提出：DSCH 已经得到发展，铺就了一条朝着更高比特速率发展的前进之路。DSCH 的引入说明空中接口具有新的增强潜力。因此，无论是出于商业还是技术方面的原因，都应该加快正在进行中开发进程。HSDPA 出现的时机已经成熟。

随后，3GPP R5 制定了新的 HSDPA 为高峰值数据速率用户提供服务。为了实现更高的数据吞吐量，降低延迟和高峰值速率，HSDPA 采用了 AMC(自适应调制和编码)和 HARQ(混合自动重传请求)，并组合使用了快速调度和快速小区切换等技术。尽管这些技术可以看作是 HSDPA 的奠基石，UTRAN 尤其是空中接口的全面增强远远超越了这些，并且不用牺牲 R4 版本的后向兼容性。

4.2.2 益处和影响

对终端用户来说，HSDPA 最大的好处是数据吞吐量能提高大约5个数量级，利用15个码字的多码，其峰值速率可以超过10Mbit/s。这个好处取决于资源配置中使用的调制技术，如图4.13所示。考虑到小区覆盖、UE 移动性、UE 到 BS 的距离、同时存在多个用户等因素会影响可实现的峰值速率，实际可达到的最大峰值速率可能会大大低于上述目标，但和 UTRAN R4 的数据能力相比还是有巨大的提高。HSDPA 增强版本的亮点还包括显著降低的端到端时延以及小区容量的提高（和 R4 中微小区的 DSCH 相比有一个数量级的提高）。这一切直接提高了系统的频谱利用率，并从根本上提高了系统的能力以适应以数据为主导的服务，它们主要集中在流媒体、交互式和后台业务而不是实时业务。

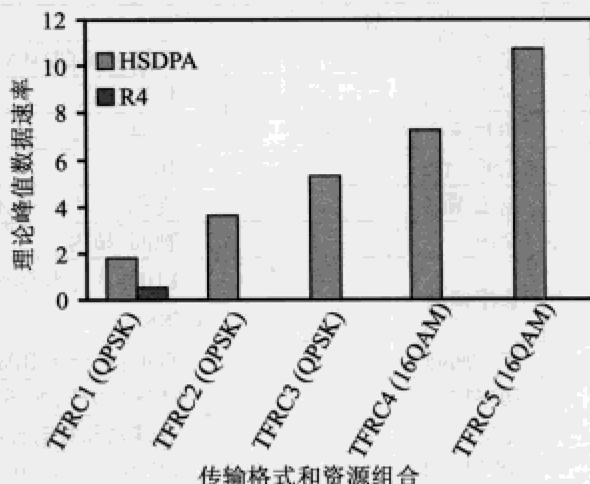


图4.13 R4 和 R5 可实现的数据速率比较

当然，HSDPA 也有其缺点：尽管保留了后向兼容性，但必须要对 R4 的空中接口和结构进行升级和改进。HSDPA 对 UMTS 网络结构尤其是其空中接口的要求可以归纳为以下几点。

- 网络结构：HSDPA 需要把大部分的分组处理功能转移到网络边缘，导致了比 R4 更分散的结构。
- 物理层：新的自适应调制和编码技术需要对物理层结构做出重大改变，包括信道结构造、复用、定时及 HSDPA 所需要的各种操作过程。
- 快速调度要求 MAC（媒体接入控制）能高效运作，并且与物理层的交互作用更为紧密。短帧要求 BS 有更高的处理能力，从某种程度上 UE 端也应如此。
- 实现快速重传要采用更多的控制信令和更先进的重传机制。

了解了这些情况之后，我们再通过对其基本概念、特性及原理的简要介绍来了解 UTRAN 中这个极具吸引力的特色。

4.2.3 基本概念

图4.14 描述了 HSDPA 的主要思想。最初，在 UMTS 的 R4 版本中，数据业务可以通过 CCH（公共信道）、DCH 和 DSCH 来处理。数据为核心的业务采用 DSCH，低速率数据可通过 FACH 和 DCH 来处理。DCH 的信道比特速率上限可通过所分配码的 SF 来相应调整。HSDPA 的主要工作就是简单地用时分复用方式在单一的共享信道上传

输数据分组,它采用多码及固定的 SF。虽然看上去简单,要实现它必须需要空中接口有一定的功能和操作流程:复用的数据要以有效的方式进行调度、调制、编码并通过在空中接口传输,并能适应于无线链路。因此,必须要在 R4 UTRAN 的特征之上进行改进。

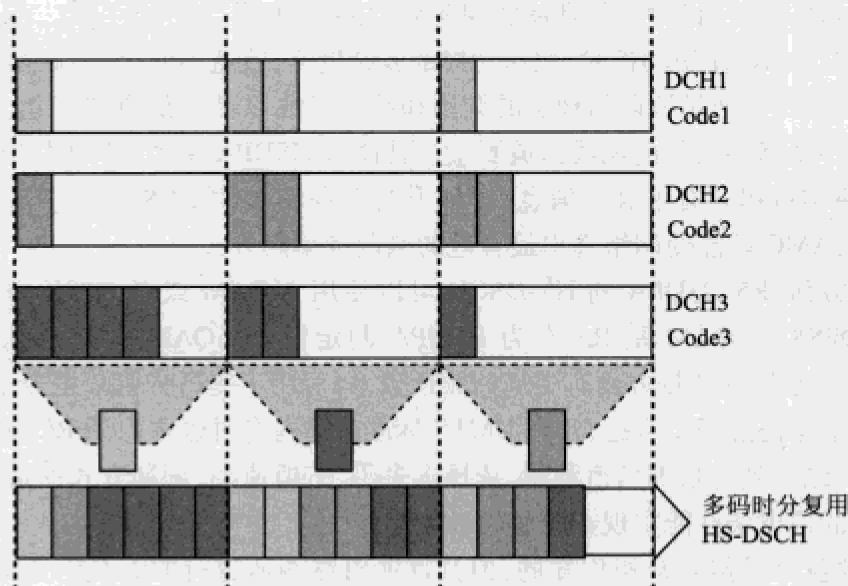


图 4.14 HSDPA 的基本原理

图 4.15 是 R5 版本为了引入上述 HSDPA 基本操作所定义的基本功能及功能实体。HSDPA 的主要功能实体包括 AMC、FPS(快速分组调度)、HARQ 以及小区切换程序,以下章节将对它们进行介绍。

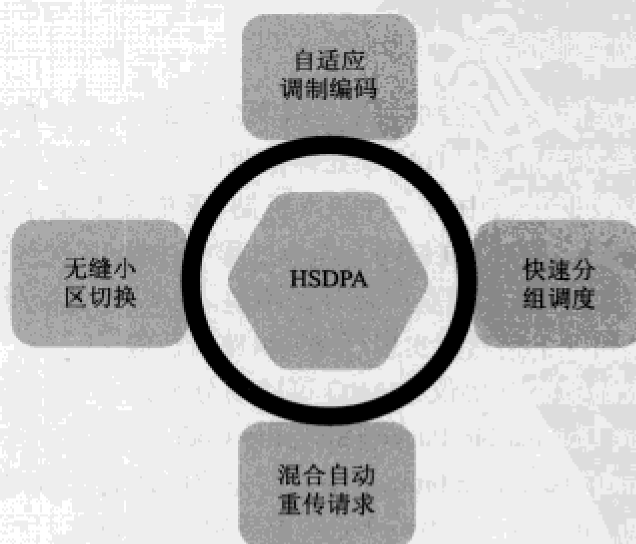


图 4.15 HSDPA 的主要功能实体

4.2.4　自适应调制编码

自适应调制编码的主要目的是通过细调传输参数来补偿无线信道的不稳定性。链路自适应的方法和手段有很多,如功率控制、自适应天线、动态码分配及信道分配等。这些技术的最终目的相同,具体实现各异,必要时可作为补充手段。不过就HSDPA而言,结合AMC使用功控时,快速功控的复杂度高,收益不明显,因此排除了功控。

AMC的主要特征是细调物理层的调制和编码参数以补偿信道的变化。完成这一点主要利用移动终端获得的无线信道测量。具体对HSDPA来说,体现为CQI(信道质量指示)和重传过程。有了这个信息,再加上与业务相关的QOS等信息,以及无线物理资源状态,AMC就能使网络选出最合适的调制和编码方式。

在调制方面,R5 HSDPA的HS-DSCH可以使用16QAM或者QPSK调制。R4标准已经有QPSK,16QAM是R5专为HSDPA制定的。16QAM这样的高阶调制与QPSK相比,在数据吞吐量方面有更高的频谱效率,可用于提高峰值数据速率。调制选择可以和信道编码过程结合进行,在UMTS标准范畴内有时也称为TFRC(传输格式和资源组合)。结果就是根据信道测量,选择出多码、信道速率、调制方式的最佳组合,从而对于特定的信道条件能实现吞吐量的最大化。

AMC的益处虽然是众所周知的,但其性能对终端所进行的无线信道测量结果很敏感:测量周期可能跟不上快衰落引起的信道变化,测量结果也不一定完全正确。如果信道状况报告不可靠,就可能做出错误的分组调度、发送功率设置、调制和编码的选择。为此,HSDPA设计了先进的CQI估计方法,它利用接收CPICH的导频功率信息、信道定时、自适应报告周期,以及高层交互来保证AMC可靠运行。此外,HARQ将链路层的信息引入这个过程,也有助于补偿AMC受到的影响。

4.2.5　混合自动重传请求

无线信道的不稳定性使得单独的直接信道测量不能为AMC的运行建立一个可靠的基础,还需采用一些补充措施。HARQ允许接收的NE(网元)检测差错并在必要的时候请求重传。作为数据传输中的一种基本机制,重传技术能保证数据包的可靠接收。与传统的ARQ相比,HARQ在链路自适应过程中,能把初次传输及重传中的直接信息或者估计值合并在一起,从而获得额外的增益。这使它能降低重传的次数,并且在无线信道有变化的情况下仍然能实现可靠的链路自适应。

根据重传时采取的策略和协议,HARQ可以划分为几个不同的版本,例如速率兼容打孔Turbo码(Rate Compatible Punctured Turbo Codes)、递增冗余Chase合并(Incremental Redundancy and Chase Combining)等。当先前的译码失败时,有些方法以递增的方式增加冗余信息,而有些方法中每次重传都是独立处理的。

由于重传时延和信令开销是最关键的指标,尤其对于移动网络应用,所以HSDPA选择了最简明的重传流程,称作SAW(停－等)。SAW持续工作在当前的分块上,直

到 UE 发回该分块成功接收的确认信息。在不需要重传时，它采用了优化应答机制和消息，以确认数据包被成功传输。为了消除等待时间引起的额外时延，采用 N 信道的 SAW HARQ 并行进行重传过程，避免浪费时间和资源。

因此，当 HARQ 协议基于异步下行链路和同步上行链路时，HSDPA 的合并方式是递增冗余。而 Chase 合并是作为 HARQ 的一个特殊版本使用的，此时上层（如 RRC 信令）把 UE 中的软存储以半静态的方式划分给不同的 HARQ 进程。这一点是靠选择和决定传输格式实现的。

4.2.6 快速调度

HSDPA 在 AMC 和 HARQ 方面的有效运行表明，分组调度可以快到能追踪 UE 衰落信号中的短期变化。在快速功控和 VSF（可变扩频因子）机制被 AMC、HARQ 和快速重传机制替代后，这一点十分重要。这也是把 PS（分组调度）放在 BTS，而不是像 R4 那样放在 RNC 中的重要原因。这样一来，调度时延大大降低，信道测量也能更好地反映无线信道的情况，从而能做出更可靠和公平的调度决定。再结合码字配置固定（16），以及 TTI（传输时间间隔）从 R4 中的 10ms 或 20ms 减到 HSDPA 中的 2ms，使得 PS 可以完成快速调度和帧成形。类似于 2G 和 3G 移动网络中 RRM（无线资源管理）算法的情节，PS 的实现也由厂商决定。

4.2.7 无缝小区切换

无缝小区切换使下行链路上的 UE 能连接到最好的可用小区，形成了 HS-PDSCH 模式下的无缝连通性。它能减少干扰，特别是软切换带来的干扰。小区切换实际上是 HS-PDSCH 移动性管理的一部分，它能保证高速率数据连接下 UE 的移动性。为了达到这个目标，服务 HS-DSCH 小区（即对于特定的 UE，在服务 HS-DSCH 无线链路上发送接收的那个 BS 所对应的小区）所扮演的角色从源 HS-DSCH 小区的某个无线链路转移到目标 HS-DSCH 小区的某个无线链路上。这里需要特别处理，因为分配给某个 UE 的 HS-PDSCH 仅属于指配给该 UE 的服务 HS-DSCH 无线链路。像 UTRAN 中普通的切换一样，服务小区的变更原则上可以由 UE 或由网络来决定。不过 R5 仅支持网络控制这个选项，它由 RRC（无线资源控制）信令处理（见图 4.16）。

服务 HS-DSCH 可以根据不同的标准和考虑来实施，包括物理信道配置、UE-UTRAN 同步及服务 BS 在网络等级中的位置。在此情形下，值得强调的是服务 HS-DSCH BS 迁移和服务 HS-DSCH 小区切换是两个不同的流程。尽管服务 HS-DSCH BS 迁移先要请求服务 HS-DSCH 小区切换，但不会反过来进行。涉及服务 HS-DSCH BS 迁移的另一个重要差别是，位于源 HS-DSCH BS 的 HARQ 实体被终止，目标 HS-DSCH BS 创建新的 HARQ 实体。不管怎样，这两个流程都通过快速的服务无线链路变更来达到 UE 在高速数据模式下的无缝连通性。

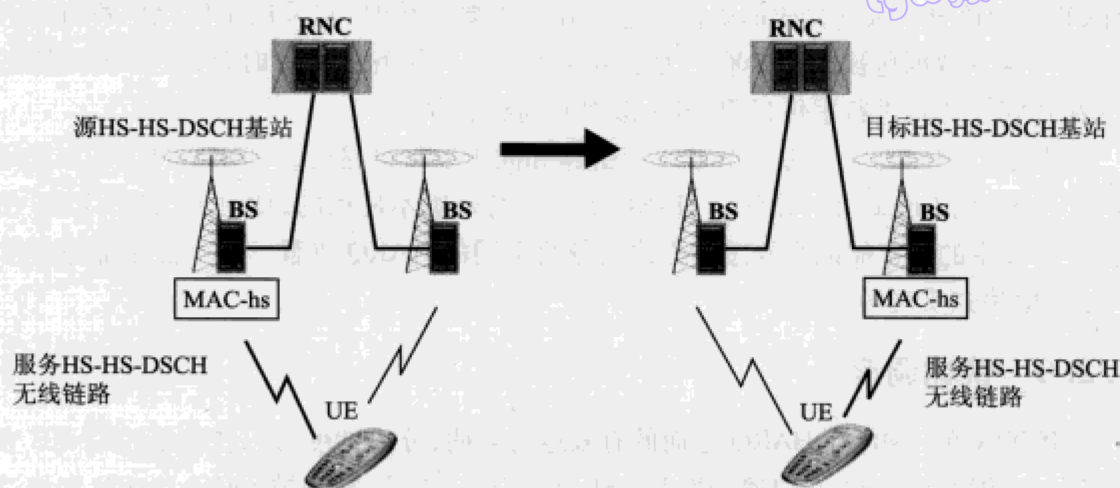


图4.16　节点B间的服务HS-DSCH小区切换，以及服务HS-DSCH节点B迁移

4.2.8　基本操作和结构问题

HSDPA的出现给BS和UE的HW(硬件)和SW(软件)模块都带来了重大的改变，尽管RNC的主要功能基本上与R4一致。图4.17示出了HSDRA实体和功能的基本流程和功能分配。最引人瞩目的是快速调度功能，已经从RNC中移到BS。除此之外，BS还负责AMC处理，比如HARQ及链路适应，这些也都是新的功能。从UE的角度来说，尽管AMC的主要功能由BS来处理，UE必须能够提供CQI和AMC信令，例如ACK/NACK消息处理以及HARQ操作模式。因此，为了能使BS和UE运行HSDPA，它们都需要升级新的属性。从RNC的角度来说，MAC-d将会被保留，MAC-hs是唯一新加到MAC层的实体。此外，还需要对RRC消息进行一些修订。

HSDPA操作还涉及三个新的信道：由多个用户共享的下行传输信道HS-DSCH，用于处理涉及译码及重传等控制信息(TFRI、HARQ)的上行逻辑信道HS-SCCH，与HS-DSCH关联、携带涉及重传(ACK/NACK)和CQI等控制信息的上行物理信道HS-DPCCH。

一个或多个HS-PDSCH与一个相关联的DPCH一起绑定到一簇独自的HS-SCCH信道上，也叫作一个“HS-SCCH”簇。这些信道之间的定时已被规定，使得HS-SCCH信息起始点与相应HS-PDSCH子帧起始点之间的时间偏移保持固定。信道配置过程由RRC信令处理。此外，UE在一个HS-SCCH簇中的信道数可以在1～4间变化。

在图4.17所示的基本HSDPA操作中，一旦RRC连接就绪，UE将向服务BS提供信道质量相关信息和其他控制信息，包括UE的能力和请求的容量。基于此信息，再结合调度相关的信息，例如所确定的TTI、无线和物理资源等，BS便可以选择HS-DSCH簇和参数、调制方式等，并且在HS-DSCH传输的两个时隙之前启动HS-SCCH传输。在接收机端，UE解出HS-SCCH信息，根据此信息(例如从TFRI中所提取的信息)获得

必要的参数，例如 HS-DSCH 传输格式的动态部分，包括传输块设置的大小、调制方案以及在相应的 HS-DSCH TTI 下的信道映射方案。一旦 UE 得到了所有需要的参数，它便开始进入数据处理以及 HARQ 处理，并返回 ACK/NACK 给 BS。完成这个过程后，HS-SCCH、HS-DSCH 和 ACK/NACK 之间的时间关系在数据连接存在期间有重要的作用，因此，UE 必须严格执行。

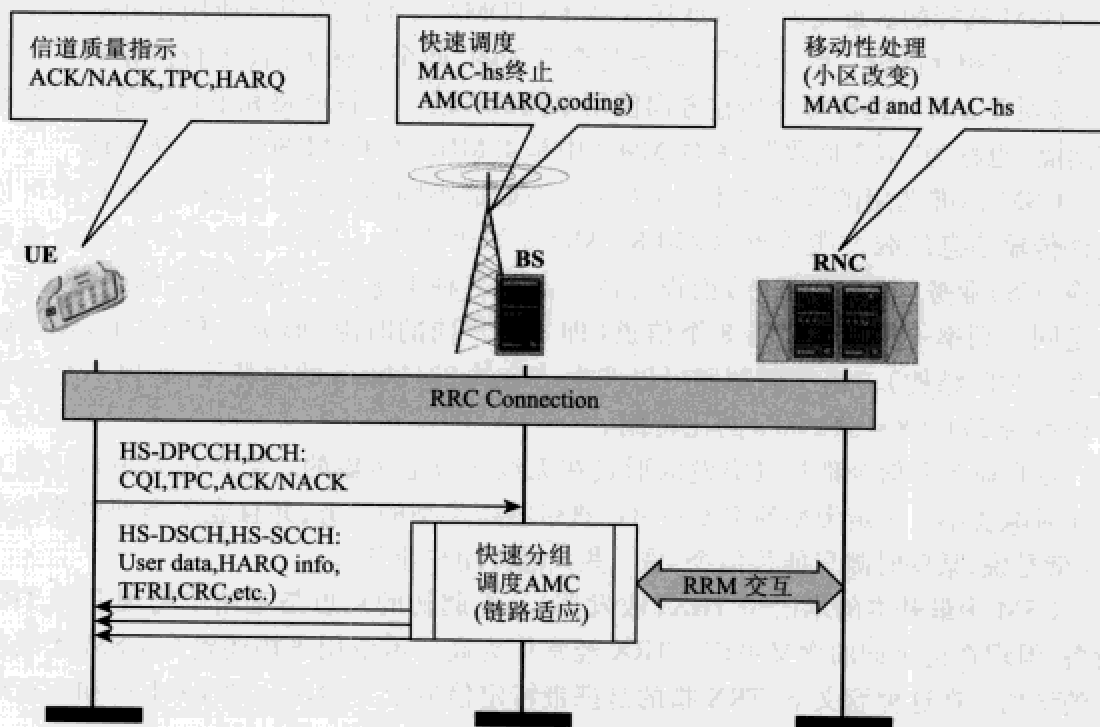


图 4.17　HSDPA 的基本流程和功能分配

4.3　GSM/EDGE

本节简要介绍 GSM 无线接入技术及其增强，通用分组无线业务（GPRS）和数据增强的 GSM 演进（EDGE）。

4.3.1　基本概念

GSM 是 20 世纪 80 年代为泛欧移动电话系统开发的无线技术。它在许多方面都标志着技术的进步。首先，它是第一个在实现之前先标准化的技术。早期技术先是在实验室中设计，然后才写出描述这个实现的“标准”。其次，和模拟无线技术相比，GSM 的设计能提供更大的容量。

由于市场上有很多详细讲述 GSM 无线通信的书籍，在这里就不作详细的讲述，只是强调一些重点。

GSM 标准最开始是在 900MHz 频段上使用，由于商业上的成功以及有必要扩展到其他频段，相同的技术经过一定修改后很快采用到其他频率上。采用原计划的频段的 GSM 第一版如今称为"GSM900"。GSM 后来使用了 1 800MHz 的频段（比 WCDMA-FDD 频段稍低），称为"GSM1800"。在美国，基于 GSM 的网络使用更高的频段，称为"GSM1900"。为了某些特殊的目的（如铁道公司），也会考虑使用其他的频段。

GSM 选择的多址是时分多址接入技术（TDMA），不同的用户使用相同的频率资源，按时间相互区分。由于 GSM 业务是全双工的，两个传输方向（上行链路和下行链路）必须要分开。这使每个传输方向使用单独的频段。上行链路和下行链路之间的频率间隔（也称为"双工间隔"）在 GSM900 中是 45MHz，在 GSM1800 中是 90MHz。

GSM 标准选用的调制技术是 GMSK（高斯最小频移键控）。这种调制技术可以允许传输信息的载波能够承载 270 833kbit/s 的比特流。GSM 系统最开始是为电路交换（CS）业务（特别是语音）而设计的。经过各种考虑以及编译码器的选择之后，决定同一频率一共可以携带 8 个信道（即 8 个不同的时隙，形成了称为"TDMA"帧的基本时间结构）。由于调制器可以产生一个约 271kbit/s 的比特流，所以一个信道可以携带 271 ÷ 8 ≈ 34kbit/s 的比特流。

用户业务和信令都是以突发的形式在无线接口上传输的。突发在大小和时间上都比时隙要小。一定类型的突发只可以携带特定类型的业务，并且业务类型也按此分开（就是说，某些时隙只能传信令，另一些只能传用户业务）。

GSM 中最基本的术语是 TRX（收发器）。它起初的意思是基站中物理上的 TRX 设备，但现在这个词的含义更广。TRX 经常作为高层术语用来描述整个 GSM 无线接口的结构。在这种意义下，TRX 指的是携带特定信道定义的两个频率（上行和下行频率）的组合（见图 4.18）。

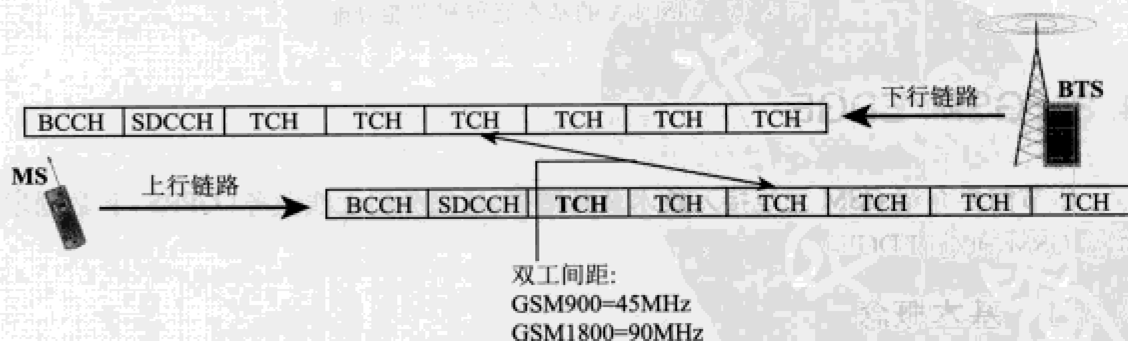


图 4.18　GSM TRX 配置示例

TRX 是最基本的术语，我们可以用它来建立起 GSM 相关的术语结构。

无线网络中，对公众而言可见性最小的部分是小区。小区的覆盖是天线结构形成的，但小区内的业务是通过 TRX 来维系的。一个小区中最少需要一个 TRX，在实际应用中每个小区一般最多有 4～6 个 TRX（见图 4.19）。

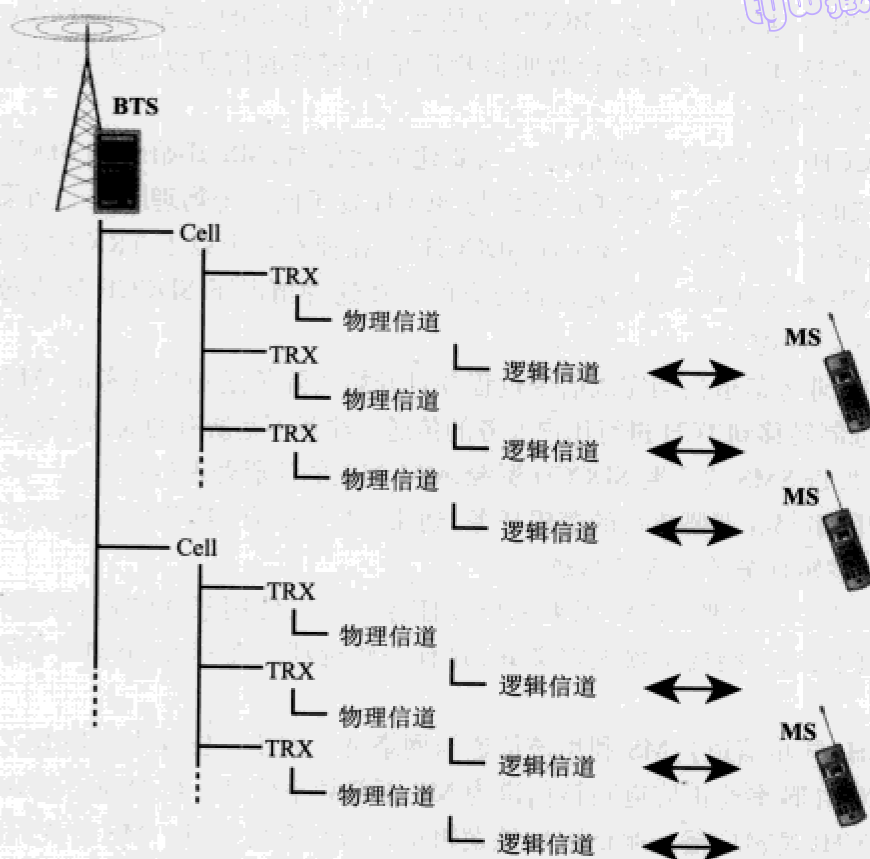


图 4.19 基站－小区－TRX 相互关系

GSM BS 是一个物理的网络单元，它可能由许多小区构成。在实际应用中，每基站至少有 1 个小区，最多有 3 个小区。

第 1 章讲述的网络资源管理模型中给出了涉及的多种管理任务和控制任务。把这个模型延伸到 GSM 系统及前述的术语中，那么 TRX 涉及无线资源，“小区”涉及移动性管理（MM）和网络寻址。移动性管理及其相关问题将在第 6 章中讲解。

4.3.2 无线信道和帧结构

因为 GSM 采用 TDMA 方式进行多址接入，所以从系统功能的角度看，网络层的同步以及不同的定时结构就显得尤为重要。基本的定时结构单元是由 TRX 维持的 TDMA 帧。

GSM 无线通信要执行很多任务，这些任务被绑定到定时结构和信道中。GSM 中的信道化系统十分简单，作为开始，它只包含两种信道类型。在无线接口中实现业务传输的无线信道称为*物理信道*。

从无线接口直到 BSC 之间都存在物理信道。由 BSC 决定它是用于传输业务还是信令。有 3 种类型的物理信道。

- BCCH(广播控制信道):BCCH 总是处于一个固定的位置,即 TDMA 帧的时隙 0(时隙从 0~7)。移动台收听该物理信道携带的信息以实现他们自身的同步并接入网络。
- SDCCH(独立专用控制信道):当要建立通信时,MS 开始使用 SDCCH 并执行相关的信令活动。SDCCH 可以与 BCCH 处于同一个物理时隙。如果是这样的话,将其合称为"组合 BCCH/SDCCH"。在拥有一个以上 TRX 的较大小区中,BCCH 和 SDCCH 通常是各自分离的。在这种情况下 SDCCH 通常位于 BCCH TRX 的时隙 1。
- TCH(业务信道):当完成信令过程并且开始实际传送用户业务时,MS 将转移或被强制转移到 TCH 进行用户业务的传送。注意不是所有的通信都需要 TCH。例如,发送 SMS 仅需要 SDCCH 资源,MM 相关的注册处理过程也是一样。

MS 和网络都有需要执行的逻辑任务,通常(不是所有)这些任务被绑定到定时结构中。这些逻辑任务称为*逻辑信道*。

逻辑信道应用物理信道资源来承担其任务。可以使用某些结构将逻辑信道捆绑到物理信道上,这些结构是预先定义好,并有一些选项。在标准 GSM 中,存在以下逻辑信道。

- SCH(同步信道):MS 利用该信道与网络进行同步。位置为物理 BCCH。
- FCCH(频率校正信道):该信道为 MS 更新频率信息。位置为物理 BCCH。
- BCCH(逻辑广播控制信道):该逻辑信道包含系统信息。MS 首先开启 SCH 和 FCH,然后读取 BCCH 信息,然后驻留在小区中。位置为物理 BCCH。
- RACH(随机接入信道):MS 利用该信道执行初始接入或其他服务(例如更新位置、语音呼叫等)。位置为物理 BCCH。
- AGCH(接入许可信道):网络使用该逻辑信道命令移动台采用逻辑 SDCCH。位置为物理 BCCH。
- PCH(寻呼信道):在移动台被叫的通信中,网络使用该逻辑信道向 MS 发送寻呼信息。位置为物理 BCCH。
- SDCCH(逻辑独立专用控制信道):根据所选信道配置,一个物理 SDCCH 可能包含 4 个或者 8 个逻辑 SDCCH 块。通信信令总会需要一个逻辑 SDCCH 块。因此,在信令阶段一个物理 SDCCH 可以同时包含 4 个或 8 个通信。位置为物理 SDCCH。
- TCH(逻辑传输信息):根据业务类型的不同,物理 TCH 可能包含多个业务信道类型,包括 TCH/F(全速率)、TCH/H(半速率)或 TCH/D(双速)。由 MS 和网络协商决定所使用的逻辑 TCH。
- SACCH(慢速随路控制信道):不论通信是在 SDCCH 上还是在 TCH 上,都要连续测量无线连接。MS 通过该逻辑信道向网络发送测量报告。SACCH 按时间绑定到 TCH 帧结构中。

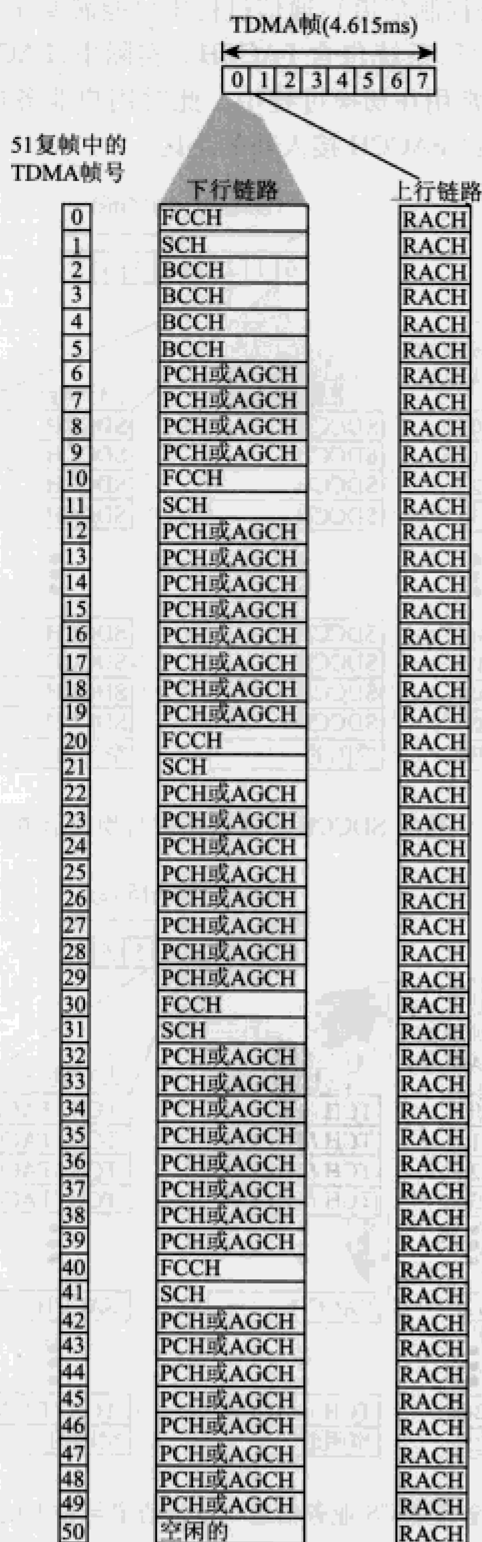


图 4.20 独立 BCCH 中逻辑信道与物理信道的映射

- FACCH(快速随路控制信道):通信过程中可能需要比 SACCH 更快地交换控制信息,在这种情况下,系统包含 FACCH。实际中,FACCH 有时会占用 TCH 的时间。FACCH 经常用在切换过程中。此时用户业务通过 TCH 传输到先前的蜂窝,同时 MS 通过 FACCH 接入新的小区。

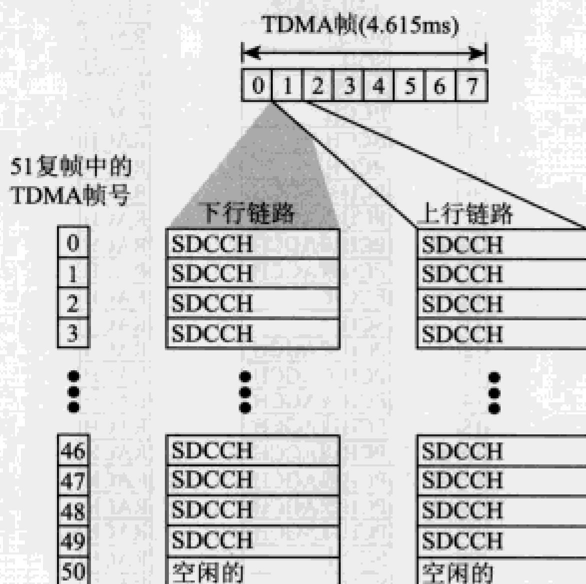


图 4.21 独立 SDCCH 中逻辑信道与物理信道的映射

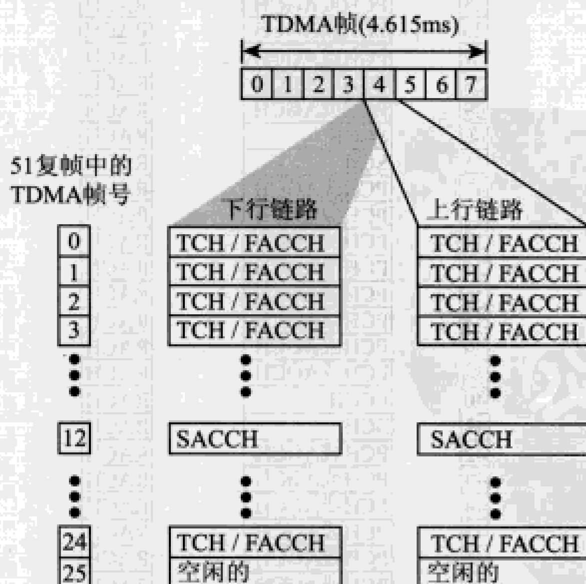


图 4.22 全速率 CS 业务信道中逻辑信道与物理信道的映射

如前所述,基本的定时结构单元是 TDMA 帧。为了组织逻辑信道和物理信道,GSM 有两种平行的帧结构。所谓的“51 帧”中包含了 51 个 TDMA 帧,这个帧结构维

持与控制跟信令相关的信道（例如物理 BCCH 和 SDCCH 遵从该结构）。在这 51 帧结构中使用物理资源的逻辑信道按特定的预定义顺序重复。系统为业务信道分配了 26 帧结构。这 26 帧定义逻辑信道如何利用物理 TCH 资源（例如，SSCCH 位于该帧结构中的什么位置）。

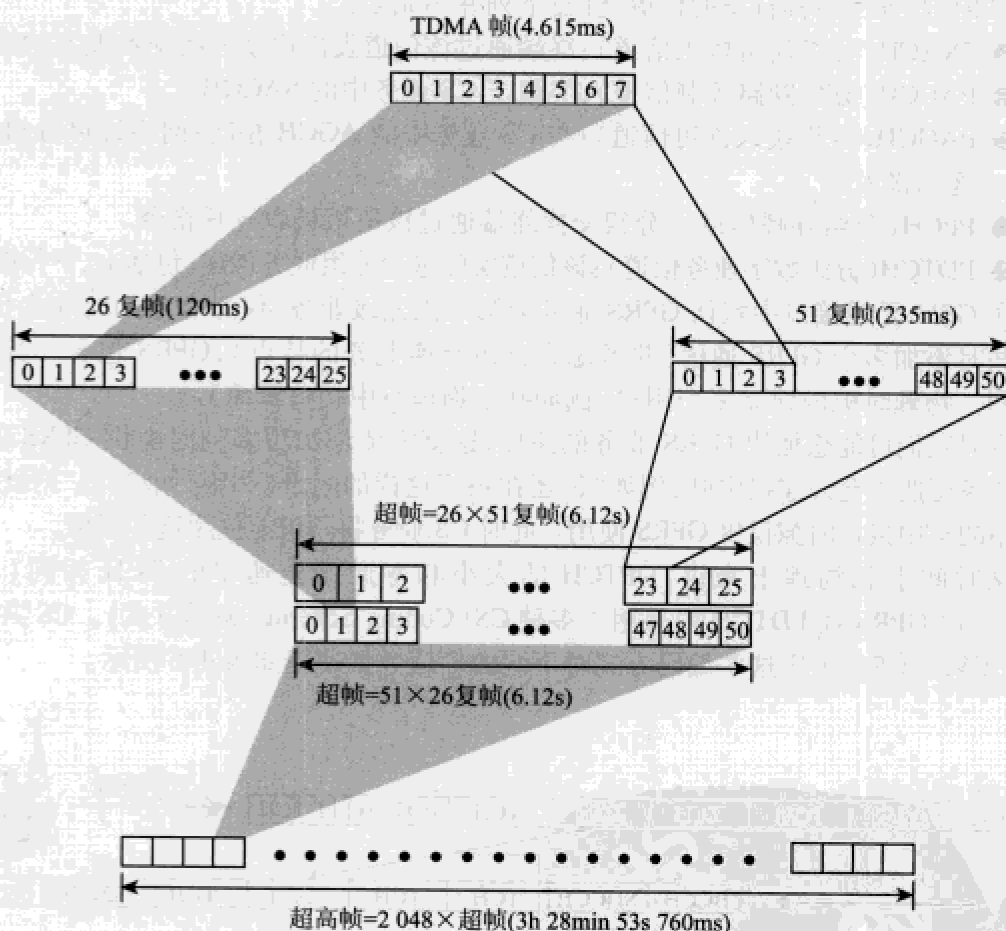


图 4.23 GSM 帧结构和定时结构

下一步就是将两个帧模型合并为一个。称其结果为“超帧”，根据情况和所选信道的不同它可能是 26 个“51 帧”结构，也可能是 51 个“26 帧”结构。

由 2 048 个超帧组成最高级的帧结构，称之为“超高帧”。超高帧也称为“密钥序列”，这是由于 GSM 无线接口的加密方法。每个 TDMA 帧由 0 开始编号，因此最大可能的 TDMA 帧号为 $26 \times 51 \times 2\ 048 - 1 = 2\ 715\ 647$。当通信转为加密模式时，网络和 MS 将协议好从哪个 TDMA 帧编号处开始加密。

4.3.3 通用分组无线业务

作为一种技术，GPRS（通用分组无线业务）是和标准 GSM 平行构建的增强技术，并利用标准 GSM 的资源。从 Um 接口来看，接口结构（时隙、定时值以及帧结构）依然

不变，但时隙的内容不同。

分组交换业务所要求的方法不同于电路交换。因此，承载GPRS业务的整个协议栈也完全不同。GPRS针对分组交换业务引入了MAC（媒体接入控制）层、RLC（无线链路控制）层以及其他一些重要的层。

GPRS业务使用其自身的信道（注意下列并不完全）。

- PRACH（分组随机接入信道）：终端通过该信道发出启动分组交换业务的请求。
- PACCH（分组随路控制信道）：类似于CS业务中的SACCH。
- PAGCH（分组接入许可信道）：与CS业务中的AGCH相同；网络许可分组交换终端接入。
- PPCH（分组寻呼信道）：分组交换终端通过该信道接收寻呼指令。
- PDTCH（分组数字业务信道）：该信道实际进行分组业务传送，包括上、下行链路。

在GSM无线接口中默认GPRS业务为第二优先级业务，仅当有空闲时才会传送。为了同时添加多个GPRS通信（并考虑到分组交换业务的特点），GPRS包含一种机制能在同一物理时隙内建立多个用户（例如共享物理空中接口资源）。

有时我们可能想加快GPRS业务的速度，这就需要增加更多的时隙供GPRS使用。有些业务可能不允许连接中断，例如"你还在吗?"这样的问讯（如银行业务）。对此可采用专用的空中接口时隙仅供GPRS使用。此时CS业务将不可能使用这些资源。

从时间上和物理上来讲，DPTCH的大小和普通的全速率的TCH相同（如图4.24）。但GPRS在PDTCH中采用了多种CS（Coding Scheme，编码方式）。CS共有四个，为CS1～CS4，采用这些编码方式时不同的信道数据速率如表4.6所示。

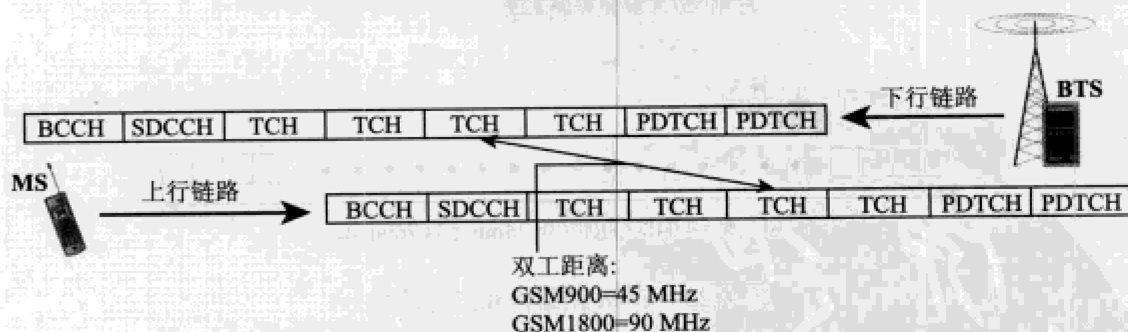


图4.24 具有两个专用PDTCH的GSM/GPRS

虽然支持GPRS的终端都支持CS1～CS4，但网络只要求必须支持CS1，其他编码方式对网络侧是选项。实际中，终端和网络都使用CS1和CS2。如果运营商想采用CS3和CS4，需要增加新的频率资源并进行仔细的规划。原因在于CS3和CS4仅在靠近天线的良好条件下才能良好运行。当终端远离基站时，干扰和其他无线接口特性将会影响无线信道的质量，使得CS更低。

表4.6 GPRS编码方案

编码方案（CS）	数据速率（kbit/s）
CS1	8.8
CS2	11.2
CS3	14.8
CS4	17.6

4.3.4　改进数据速率 Global/GSM 服务(EDGE)

从前一小节可以看出,GPRS 的问题在于数据速率。对于怎样提高 2G GPRS 平均数据速率的问题,EDGE 包含了问题的答案。从技术上来说,需要 3 个实体来实现 EDGE。

- 新的调制 8 进制移相键控方式(8 PSK):它可显著提高 GMSK 的容量。
- 新的调制编码方案(MCS):新的信道编码能使同样大小的物理时隙内可携带更多的比特。
- 无线和传输网络规划。

和 GPRS 一样,引入 EDGE 后,就时间和帧而言,无线接口的物理结构保持不变,EDGE 带来改变只在时隙内。新的 MCS 允许的数据速率如表 4.7 所示。

表 4.7　EDGE 的调制编码方案及数据速率

MCS	调　制	数据速率(kbit/s)
MCS1	GMSK	8.8
MCS2	GMSK	11.2
MCS3	GMSK	14.8
MCS4	GMSK	17.6
MCS5	8-PSK	22.4
MCS6	8-PSK	27.2
MCS7	8-PSK	44.8
MCS8	8-PSK	54.4
MCS9	8-PSK	59.2

MCS1-MCS4 与 GPRS 中的 CS1-CS4 相同。EDGE 所增加的是 CS5-CS9。数据速率越高,系统所见的比特流就越少(MCS 越高则差错保护越少)。

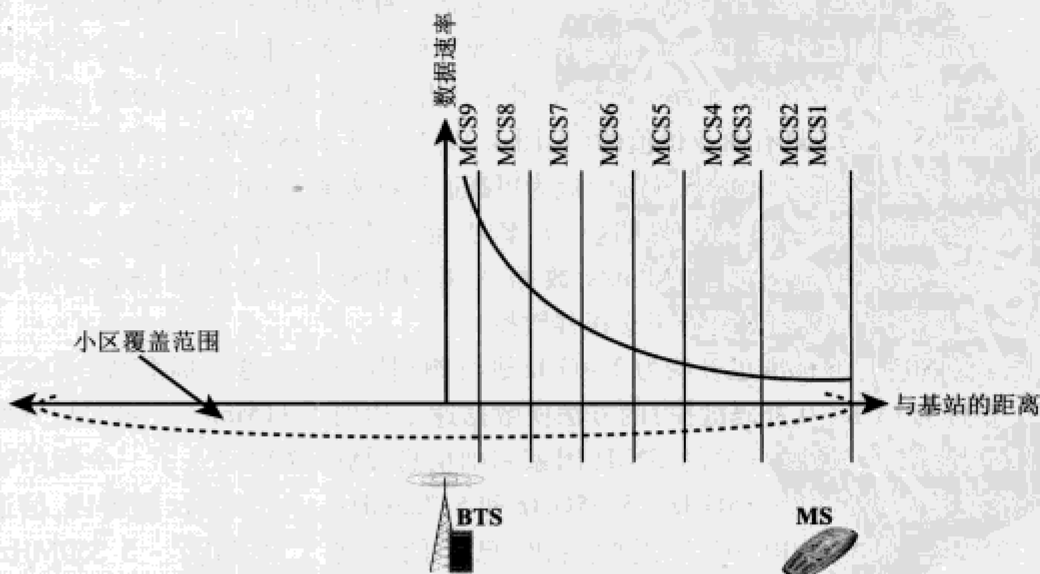


图 4.25　MCS 与离开 BS 的距离

因此，只有当无线环境很理想，一般如非常接近天线时，才会使用最高级的MCS。最低别的MCS1和MCS2在整个小区覆盖范围中都可用。

如果运营商打算提供需要更高的MCS(如MCS6或MCS7)的更高平均数据速率，那么无线网络就要进行重大改变。在整个网络范围内实现更高级别的MCS势必导致小区更小。因而在相同覆盖范围内需要更多的小区。换句话说，提高平均数据速率将增加网络中小区的数量。若想在整个覆盖区内都能使用最高级别的MCS，小区数量的增加将会非常大。

另一个问题是传输网络。如果径由无线接口的用户数据速率增加了，传送网络就必须考虑这个因素。这种现象首先出现在MCS4中，因为MCS4数据速率超过了标准GSM Abis信道(BTS-BSC接口)所能承载的数据量。

4.4 WLAN技术

本节介绍作为3GPP补充接入技术的WLAN技术。常称为"WLAN"或"Wi-Fi"(无线保真联盟，其任务是促进和验证基于IEEE 802.11的商业产品的互操作性和兼容性)的商用技术的基础是IEEE 802.11标准系列。尽管IEEE 802.11无线技术最早是为了代替LAN(有线局域网)和扩充因特网而发展的，它也逐渐变成接入UMTS网络的一种补充技术。最近，3GPP已着手研究UMTS网络与802.11系列标准的互通问题，以通过广域网蜂窝网络来支持热点应用，或者反之。

4.4.1 物理层技术

最初在1997年通过的IEEE 802.11标准主要致力于开发WLAN的无线和链路层。在这方面，IEEE 802.11系列定义了一个包括三种物理层选项的无线技术。这一无线标准包括散射红外线、DSSS(直接序列扩频)和有三种不同跳频集的FHSS(跳频扩频)，每个跳频集包含26个跳频序列。其中工作在2.4GHz工科医(ISM)频带内的DSSS和FHSS是迄今最有商业价值的(见图4.26)。由于FHSS方案在支持高速(高于2Mbit/s)时存在一些限制，DSSS实际上成为更高速比特速率应用的主流物理层技术。

如同传统的DSSS，WLAN使用这一方案时，也是在TRX中用高速的伪随机序列对数据流进行调制和解调。1Mbit/s数据使用DBPSK(二进制差分相移键控)。2Mbit/s数据使用DQPSK(差分正交相移键控)。

后来的802.11b标准也开始为2.4GHz进行物理层开发。这个标准结合DSSS采用了一种称为CCK(互补码键控)的方法使数据速率达到了11Mbit/s。再之后开发的802.11a新标准在5GHz开放的UNII(国家基础信息设施)频段引入了一个新的物理层，工作在美国分配的5.15GHz～5.35GHz和5.725GHz～5.825GHz频带内，信道间隔是20MHz。根据WRC-03最近的结果，已经同意将5 150MHz～5 350MHz和5 470MHz～5 725MHz的频带作为802.11标准的频段进行全球协调。

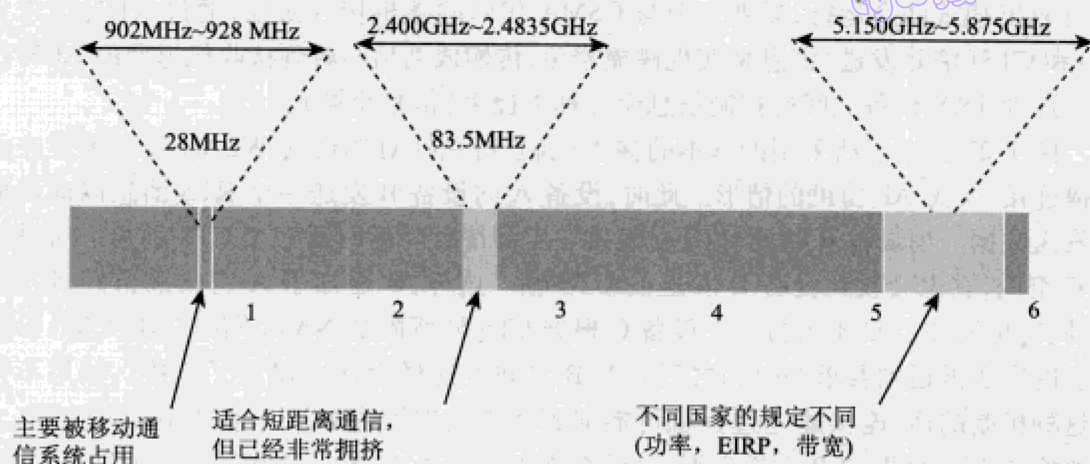


图 4.26 WLAN 可用的开放频段

802.11a 的技术基础是 OFDM(正交频分多址)，它能进一步提高对抗无线信道中有害因素的能力。尤其当配置了卷积码和比特交织时，OFDM 能够有效解决多径传播问题。另外，802.11a 使用了 AMC。这些技术在组合上 BPSK 和 64 进制 QAM(正交幅度调制)后，能使物理层提供最高达到 54Mbit/s 的比特速率。工作在 2.4GHz 的 802.11g 标准也利用了 OFDM 及 PBCC(二进制分组卷积码)，进一步提高了无线传输的健壮性。表 4.8 是 802.11 标准最基本参数的总结。

表 4.8 802.11 无线技术的关键参数

参 数	802.11	802.11b	802.11a	802.11g
频率	2.4GHz	2.4GHz	5GHz	2.4GHz
比特速率	1Mbit/s ~ 2Mbit/s	1Mbit/s，2Mbit/s，5Mbit/s 和 11Mbit/s	6Mbit/s，12Mbit/s，24Mbit/s 和 54Mbit/s	54Mbit/s
物理层	IR，DSSS，FHSS	带 CCK 的 HR/DSSS	OFDM	OFDM，PBDD
时隙	20μs	20μs	9μs	20μs 或 9μs
调制	DS-DBPSK，DS-DQPSK	DS-DBPSK，DS-DQPSK，PBCC	BPSK，QPSK，QAM	DS-DBPSK，ERP-OFDM，PBCC
范围	50 ~ 100m	50 ~ 100m	50 ~ 100m	50 ~ 100m

4.4.2 媒体接入控制

WLAN 采用了带碰撞避免的 CSMA/CA(载波监听多址接入)的 MAC 层，它能够处理信道分配、PDU(协议数据单元)的寻址、成帧、错误检测、安全、功率管理、同步和数据封装。MAC 层有两种模式，分别是基于优先级/轮询的 PCF(点协调功能)和基于竞争的 DCF(分布式协调功能)。PCF 模式通过允许 AP(接入点)在 BSS(基本服务集)或者覆盖区域内轮询终端，来提供一个小区式的网络环境。DCF 模式则是基本的接入方法，它支持尽力而为方式的数据传输和对等自组织类型的通信。DCF 模式也可

以与PCF模式联合运行，提供一个与CSMA相似的随机接入协议，通过RTS（请求发送）和CTS（清除发送）消息来实现碰撞避免，传输成功后会收到接收机返回的ACK信息。这种TRX设备之间的控制信息交互称为握手（信号交换）。

图4.27示出了所采用的基本的握手机制，特别针对邻近的WLAN设备欲建立无碰撞连接，又无AP协助的情形。此时，设备A向设备B发送一个RTS消息以确认能否发送数据。当设备B收到RTS并经过一定等待时间后回复一个CTS消息。假设设备C空闲，它也会收到设备B发送的CTS帧。这样，B通知了A它已准备好接收数据，同时也通知了C不要打扰。设备C根据CTS帧所附的NAV（网络分配矢量）参数将它的发送推迟到要求的时间之后。A、B之间就这样成功地建立了连接。如果不使用这种机制的话，连接建立过程就可能遇到所谓的"隐藏效应"。假设在这个时候，C也要像A那样试图向B发送数据，自然会在B处产生碰撞。虽然基本的RTS-CTS握手可能会出现所谓的"暴露效应"（例如，C也被阻止向A、B以外的设备发送），它毕竟大大减轻了隐藏问题。

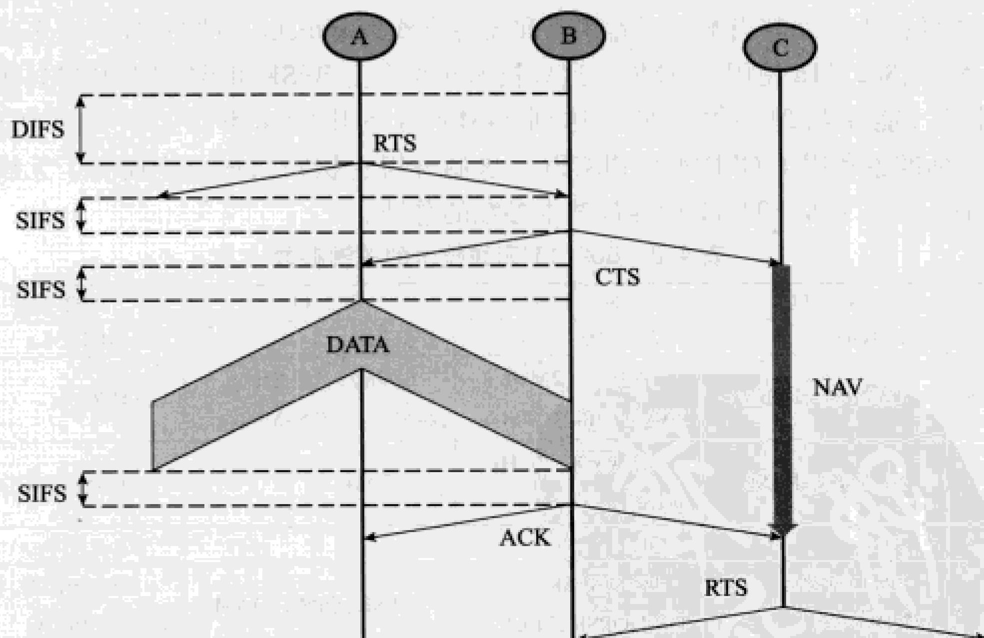


图4.27　802.11中使用的握手和载波监听过程

WLAN中的载波监听可以在物理层或者MAC层，分别称为CCA（清除信道分配）和"虚拟载波监听"。前一种情况中只有基本的RTS-CTS，后一种情况如图所示，是给RTS-CTS对扩展了一定的时延。除了基本的CSMA/CA特征和握手机制之外，MAC使用了不同的基于时延的技术和参数：例如，IFS（帧间间隔）和NAV参数用于控制接入的优先级以及MPDU（MAC协议数据单元）的成功传输。采用NAV和CCA指示信道耗用时间和后退周期后，MAC使用了三种类型的IFS。

- SIFS（短帧间间隔）。

- PIFS(端对等功能帧间间隔)。
- DIFS(DCF 帧间间隔)。

MAC 支持三类帧:管理、控制和数据。其中管理帧用于处理终端与 AP 间的联系与重联系、定时与同步、以及鉴权与去鉴权。控制帧用于 RTS-CTS 握手、肯定性 ACK,以及竞争模式之间的转换(CP 和 CFP)。数据帧可用于 CP 或 CFP 模式。在 CFP 模式下,数据帧可以和轮询或 ACK 结合。

MAC 帧格式是变长的,包含有效负荷和加密/解密字节用于可选的 WEP(有线等效协议)。WEP 及其最新进展形成了 802.11 的基础安全方案。WEP 的运算法则基本上用来加密 802.11 各部分间的信息交换,某种程度上说是为了对等鉴权。

IEEE 标准中的48 位 MAC 地址用于源和目的设备识别。为了方便 WLAN 覆盖范围内的移动性,进一步定义了 TA(发射机地址)、RA(接收机地址)和 BSSI(基本服务集识别)。留有一个位置来标示帧类型是控制、管理还是数据。另外,采用循 CRC(环冗余校验)进行错误检测。同步的处理依靠定时信标和 AP 参考时钟。这个信标还用于终端在唤醒和轻度休眠状态之间转换发送功率。

为了降低 WLAN 设备的功耗,802.11 标准还引入了一个电源管理机制。这里定义了两种运行模式:即 CPM(连续工作模式)和 PSM(节电模式)。在前一种模式中,设备连续给 AP 或相邻设备报告其状态信息,在后面一种模式中,设备只在唤醒状态时传递信息。这样,WLAN 设备就能显著降低电耗。

4.4.3 网络构成

关于接入结构,WLAN 接入网包含一个 AP 和 AP 直接控制下的一系列终端。这些形成了 BSS(基本服务集),也称为接入网的 BSA(基本服务区)。AP 的主要功能是控制网络,建立起无线和有线 LAN 的桥接。AP 很像是蜂窝网中的 BS。当存在 AP 时,终端并不与其近邻进行对等通信,而是形成一个集中控制的星型网络拓扑结构。所有终端之间的通信,或者终端与有线网客户之间的通信都要通过 AP。起初 AP 的设计并没有考虑支持终端的移动性,但在一定程度上能支持携带式的移动性。便携设备能够漫游于 AP 间,这样就能实现无缝的本地覆盖。如图 4.28 所示,按这种配置工作的 WLAN 网称为工作在“架构模式”下。



图 4.28 802.11 接入网的基本结构

IEEE 802.11 标准除了能支持架构模式外，一定程度上也能支持自组织配置。自组织模式不一定需要固定的 AP。而是"选取"一个节点来作为主节点，形成一个局域网，其他节点成为从节点。任何节点能够处理主节点的逻辑功能。因此，邻近的节点之间通过直接的无线链路通信，同时又能共享主节点的小区覆盖范围。不过这种以自组织方式形成的 WLAN 存在这样一些严重的制约：单一的共享信道、缺少多跳路由、存在隐藏和暴露效应，再加上不能通过多跳安全而有效地传送 TCP（传输控制协议）业务。

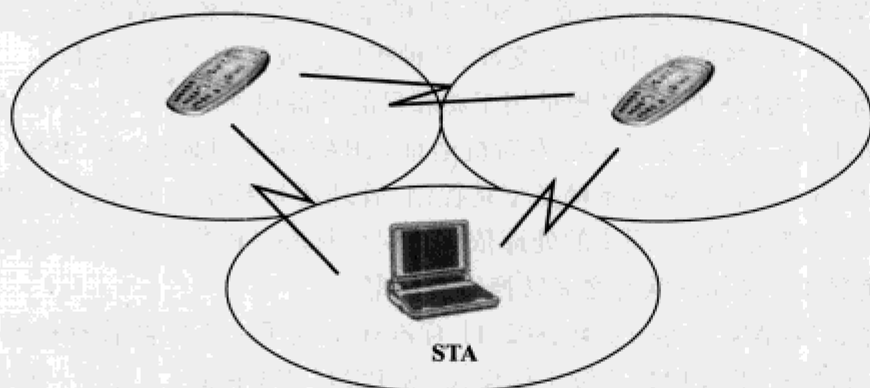


图 4.29　以 STA 为唯一构建模块的 IBSS（独立基本服务设置）

WLAN 的发展迅速超越了原先设想的热点区域，迫切需要针对居民区和企业提出增强版本。这导致了标准的发展，主要差别在于使用的频率、数据速率和调制方法。虽然互操作性也是一个问题，标准化过程也已有所考虑，标准的进一步无疑会使某些标准出现不能后向兼容的问题。随着 WLAN 取得空前成功，基本标准也遇到了新挑战。其结果是，标准化过程也将持续进行以满足各种不同的需求（如 QoS、安全、使用外部网连接 Internet、无线资源测量、切换和快速漫游等）。

第 5 章 UMTS 无线接入网

尽管通用移动通信系统(UMTS)正快速向全多址接入网络发展,但是 UTRAN(UMTS 地面接入网)已经形成其主要的 RAN(无线接入网络)。UTRAN 的主要功能是建立和维护 UE(User Equipment,用户设备)与 CN(Core Network 核心网)间用于通信的 RAB(Radio Access Bearer,无线接入承载)。RAB 使核心网单元粗略有了一条到达 UE 的固定通信路径,从而可以使得核心网单元不必再顾及无线通信方面。参考第 1 章给出的网络体系模型,UTRAN 使得 QoS 的一部分可以独立发生(见图 5.1)。

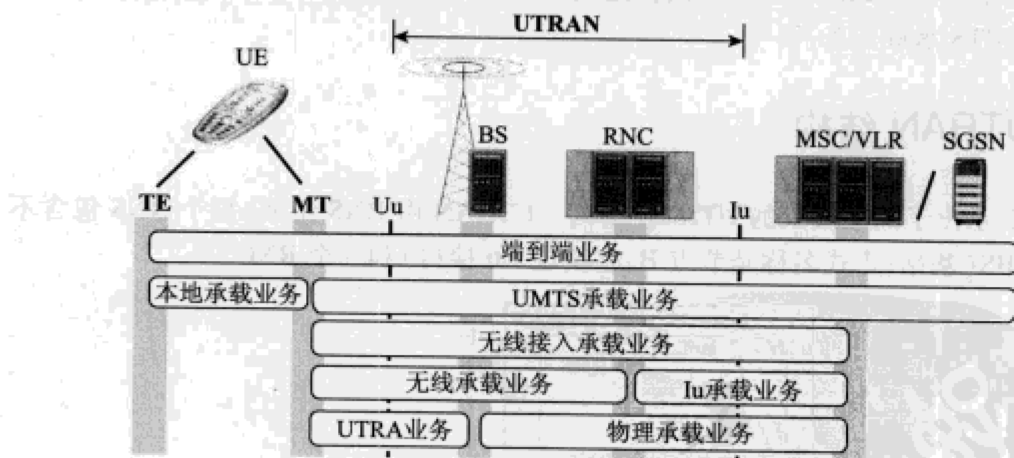


图 5.1　UTRAN 中的承载和 QoS 体系

UTRAN 位于两个开放接口 Uu 和 Iu 之间,从承载体系来看,UTRAN 的主要功能是在这些接口上提供承载业务,也就是说,UTRAN 控制 Uu 接口,并且与 CN 一起合作在 Iu 接口提供各种承载业务。

RAB 用来实现由 CN 设置的 QoS 要求,通信管理模块用来负责处理 UE 和 CN 中端到端的 QoS 要求。这些 QoS 要求映射到 RAB,它对 CN 和移动终端(MT)是可见的。如前所述,UTRAN 的主要功能是建立和维护 RAB,以便端到端的 QoS 要求在各方面都可以实现。

这种层结构的主要考虑之一是封装物理层的无线接入功能,这样,以后可以在不改动整个网络的前提下对它进行修改或替换。另外,大家都知道无线路径是一种非常

复杂且不断变化的传输媒介。这样的承载体系对 RNC(Radio Network Controller,无线网络控制器)起着很重要的作用,因为 RNC 和 CN 一起把端到端的 QoS 要求映射到 Iu 接口,RNC 负责无线路径中的 QoS 要求。在系统中之所以同时存在这两种承载是因为 Iu 承载本质上非常稳定,而 RAB 在连接过程中变化较大。例如,一个 UE 和 RNC 之间可能同时存在三个不断变化的 RAB,而 RNC 对此只有一个 Iu 承载。这种情形主要发生在软切换状态,本章将会对此进行详细介绍。

由 Uu 接口提供的端到端业务的物理基础是 UTRA(Universal Terrestrial Radio Access)业务。如第4章所述,UTRA 业务采用 WCDMA 无线技术实现,初期采用 WCDMA-FDD(频分双工)模式。从 QoS 看,UTRA 包含有如何将端到端的 QoS 要求映射到物理无线信道的机制。UTRAN 中每一个 Uu 接口连接在固网侧都分别有一个对应接口,对等的固网侧物理基础是 PBS(物理层承载业务)。它可以通过很多技术来实现,但 3GPP R99 中最可能的选项是在物理传输媒介中采用 ATM(Asynchronous Transfer Mode,异步传输模式)。本书的第10章介绍 ATM 和其他物理层传送技术。随着 UTRAN 的演进,IP 将会作为另一种实现方式替代 ATM(见第2章和第3章)。

根据第1章讲述的概念模型可知,实现 RB 业务的协议属于接入层(RB 是 RLC 层提供的业务,用于在 UE 和 RNC 之间传送用户数据)。RB 业务之上的协议属于非接入层,负责 UMTS 承载业务。

5.1 UTRAN 结构

图5.2示出了网元级别的 UTRAN 结构。UTRAN 由 RNS 组成,每个 RNS 包含不同数量的 BS(基站,正式名称是节点 B,它实现 Uu 接口)和一个 RNC。

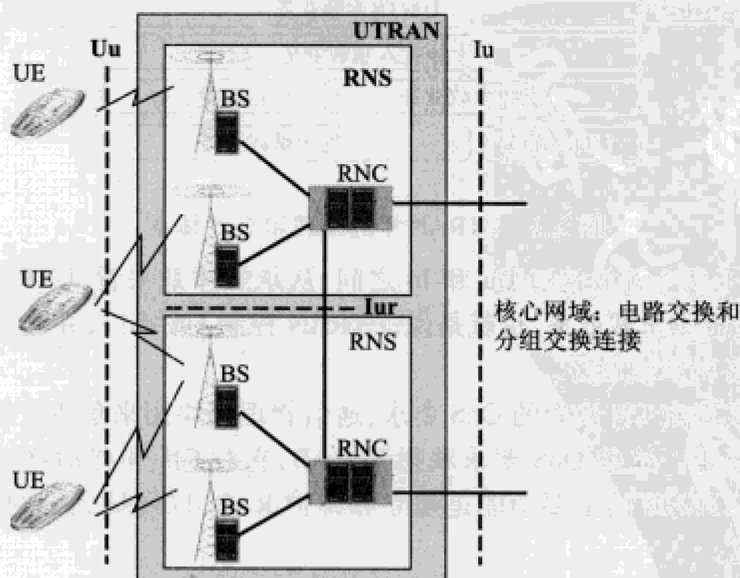


图5.2 UTRAN 的一般结构

不同的RNS由UMTS接口分开,这些Iur(接口)位于RNC之间并形成RNC间的连接。Iur是一个开放接口,能传输信令和业务信息。

5.2 BS

BS位于Uu和UMTS接口之间,而UMTS接口位于RNC和BS(Iur)接口之间。对于用户终端而言,BS的主要任务是实现Uu接口的物理功能,而对于网络端而言,BS的主要任务是通过为这些接口定义协议栈来实现Iub接口的功能。通过Uu接口,BS可以实现WCDMA无线接入物理信道的功能,并且能把来自于传输信道的信息根据RNC的安排传输到物理信道,如第4章所述。

5.2.1 基站结构

BS可以看作是UTRAN的无线边缘,因此其基本任务是进行无线信号的接收和发送(Rx和Tx)、滤波与放大、调制和解调以及对RAN的接口。BS的内部结构由厂商决定,但基本上都由图5.3所示的组件构成。

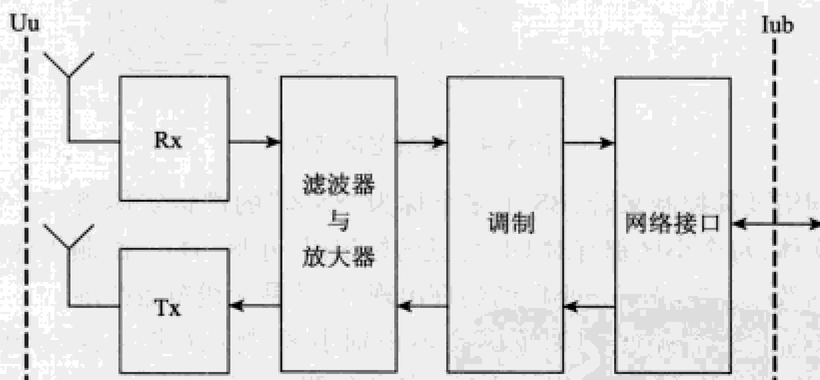


图5.3 BS基本结构

它的逻辑结构(即UTRAN处理BS的方式)是一般性的。从网络的观点来看,BS能够分成几个逻辑实体,如图5.4所示。

在Iub端,BS是两种实体的组合:包括公共传输和许多TTP(业务传输终点)。公共传输是一个小区中所有用户共同使用的传输信道和用于初始接入的信道。公共传输实体也包含一个用于O&M(运维)目的的节点B控制端口。每个TTP由许多节点B通信报文组成。节点B通信报文又由专用模式UE所要求的专用资源组成。因此,一个节点B通信报文至少包含一个DCH(专用信道)。例外是DSCH(下行共享信道)和HS-DSCH(高速DSCH),它们也属于节点B通信报文。从UMTS网络的架构来看,BS可视为网管操作中的一个逻辑运维实体。此时它描述的是物理基站及其环境(站址)。

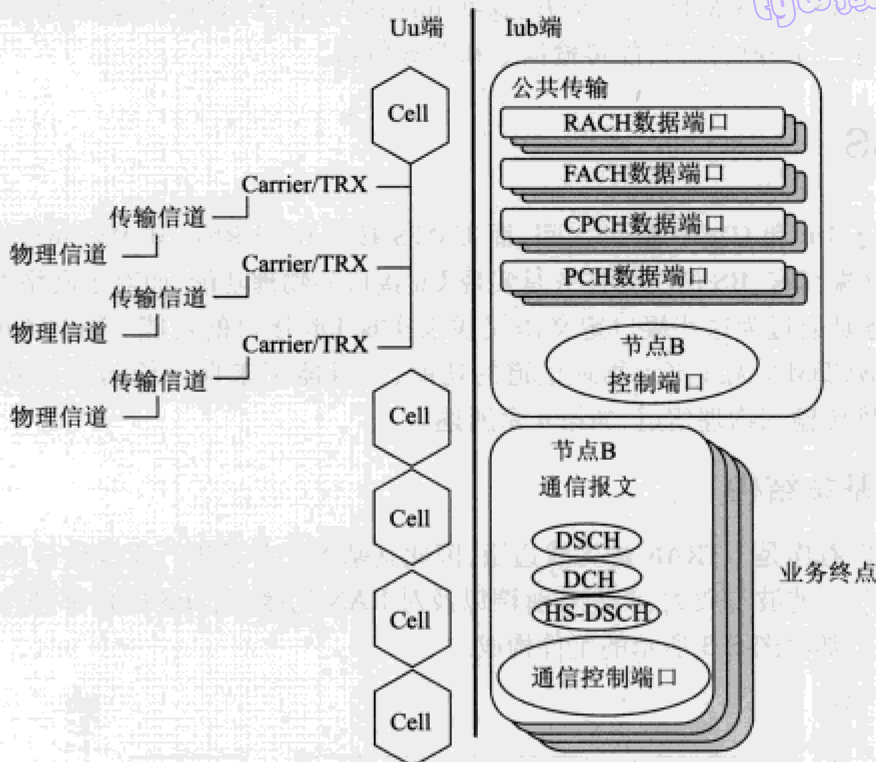


图 5.4 基站逻辑结构

从无线网络及其控制来看，BS 由多个称为“小区”的逻辑实体组织。小区是最小的无线网络实体，每个小区都有对 UE 可见的标识码（小区 ID）。配制无线网路实际就是改变小区的数据。“扇区”是小区的物理出现，也就是无线覆盖范围。

每个小区都有一个扰码。UE 靠两个值识别小区：扰码（进入小区）和小区 ID 号（用于无线网络拓扑结构）。一个小区可能有多个 TRX（Transmitter-Receiver，收发器）。小区的 TRX 把广播信息发送给 UE，即发送包含了 BCH 信息的 P-CCPCH（主公共控制物理信道）。TRX 维护通过 Uu 接口的物理信道，这些物理信道上是携带实际信息的传输信道，这些信道可能是公共信道，也可能是专用信道。

一个小区至少要包含一个 TRX。TRX 是基站实现各种功能的物理部件，这些功能比如是从地面 Iub 连接到无线通道数据流的转换，或者反之。

5.2.2 调制方式

从系统来看，所用调制方式与系统的容量和性能紧密相关。WCDMA 使用的调制方式包括 QPSK（正交相移键控）及其变型双 QPSK 和 16QAM（16 进制正交幅度调制）。QAM 结合 AMC（自适应调制编码）及 HARQ（混合自动重传请求）成为 3GPP R5 标准 WCDMA 的重要特点，与之关联的是 HSDPA（高速下行分组接入）增强。有些信道使用 QPSK 调制，如下行物理信道 P-CCPCH、S-CCPCH、CPICH、AICH、AP-AICH、

CSICH、CD/CA-ICH、PICH、HS-SCCH、PDSCH 和下行 DPCH，但下行物理信道 HS-PDSCH 可根据请求的比特速率和无线信道条件决定使用 QPSK 或 16QPM。

QPSK 调制用不同的载波相位来表达每个比特的状态。调制过程比特是成对处理的，这样就产了四种可能的 2bit 组合信号。

如图 5.5 所示，QPSK 调制先将物理层信道从串行转换成并行格式。然后把数据流分成 I 和 Q 路两路。在 I 路，比特值为 1 代表 +180°相移，比特值为 0 代表载波相位不变，在 Q 路，比特值为 1 代表 +90°相移，而比特值为 0 则代表 −90°相移。两个支路都连着振荡器，I 路是直接连，Q 路经过了 +90°相移。当输入数据流与振荡器的输出合并时，所得的 2bit 组合（1bit 来自 I 路，另外，1bit 来自 Q 路）代表图右所示的相移。图中细线表示系统中状态（相位）可能的转移“路径”。

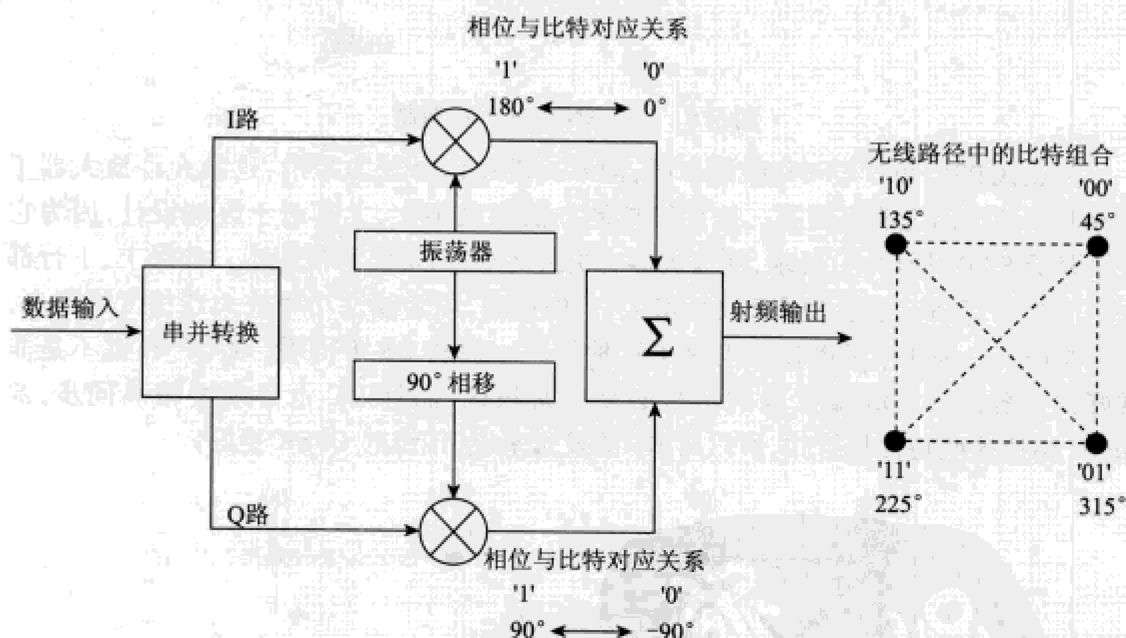


图 5.5 QPSK 调制的主要原理

以上系统能够很好地工作，不过某些 2bit 组合会带来一些麻烦。例如，当比特值由“00”变化为“11”时，将有 180°的相移，意味着有显著的幅度变化。过大的幅度变化会产生一些问题，特别是在无线连接中使用的带宽很宽时。在这种情况下，为了保证在整个带宽内都能正确地反映出幅度变化，基站必须采用线性放大器。

为了消除振幅急剧变化的影响，可以采用 QPSK 的一种变型，即 dual QPSK（双信道正交相移键控）。其结果是 DPCCH（专用物理公共信道）和 DPDCH（专用物理数据信道）不再是时间复用，而是复数扰码的 I/Q 码分复用，如图 5.6 所示。同时调制器的 Q 路引入了 0.5bit（码片）的时延（见图 5.7），以避免 180°相移，使相移限制在 90°变化。这样，原先“11”到“00”的迁移现在变为“11”—“10”—“00”，并且发生在同一 QPSK 的时间帧内。

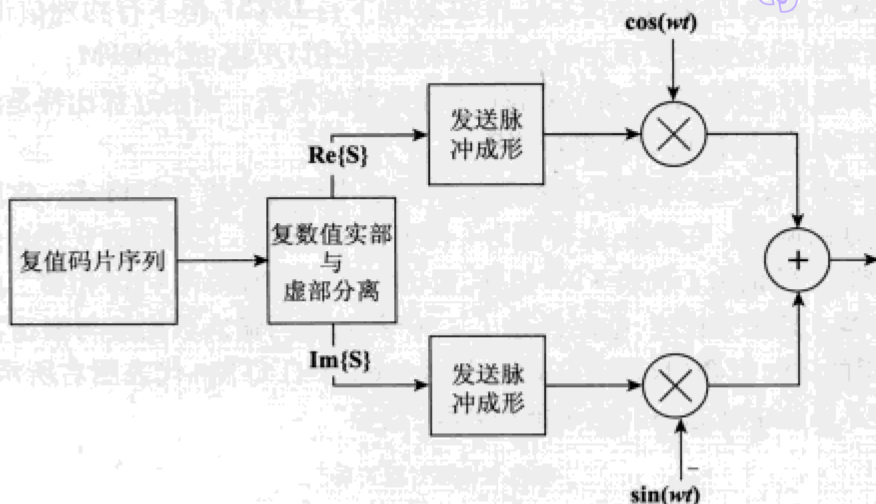


图 5.6　UTRAN 中的上行调制

因此，QPSK 和双 QPSK 频谱相同，但双 QPSK 信号较为平滑，这就允许放大器工作在非线性区而无明显问题。这种简单的办法意义很大，尤其对于终端设计，因为它能够降低 PAR(峰均比)要求，使放大器有更大的功率，最终降低成本。如果上、下行都采用传统的 QPSK，就会使 UE 功耗增大，价格更高，因为线性功率放大器精度要求高，所以很昂贵。使用双 QPSK 就消除了这种问题。但从 BS 方面看，双 QPSK 就不是非常好的方案，因为 BS 端发送的信号必须非常精确，而且 UE 也必须要精确同步，双 QPSK 会使这些特性打折扣，所以对 BS 的发送来说，传统的 QPSK 更好。

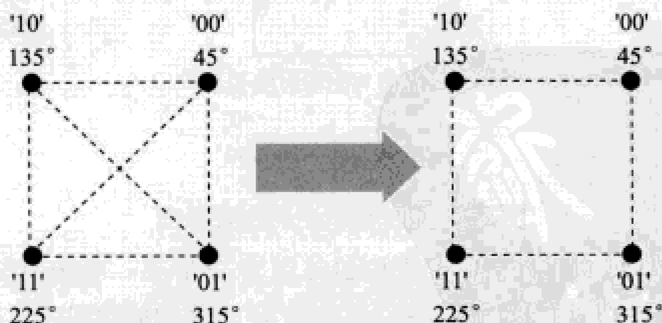


图 5.7　上行调制组合 I/Q 码分复用的结果

除了 QPSK 和双 QPSK，WCDMA 还使用了 QAM 调制，如 4.2 节所述，WCDMA R5 版本为了 HSDPA 数据增强采用了这种调制技术。这种过渡很容易理解：HSDPA 的主要目标就是达到比 3GPP R4 更高的比特速率。完全采用 QPSK 并不能有效达到目标的比特速率。与 QPSK 只利用相位信息不同，QAM 在信号星座图中充分利用了相位和幅度信息。这样，如图 5.8 所示，就可以根据采用的调制级数来成倍改进数据速率。QAM 用两个载波差 90°的支路在物理信道中发送数据。90°相移和正交载波使每一路可以独立进行调制和发送，终端也可以分别解调(如应用于 HSDPA 中)。

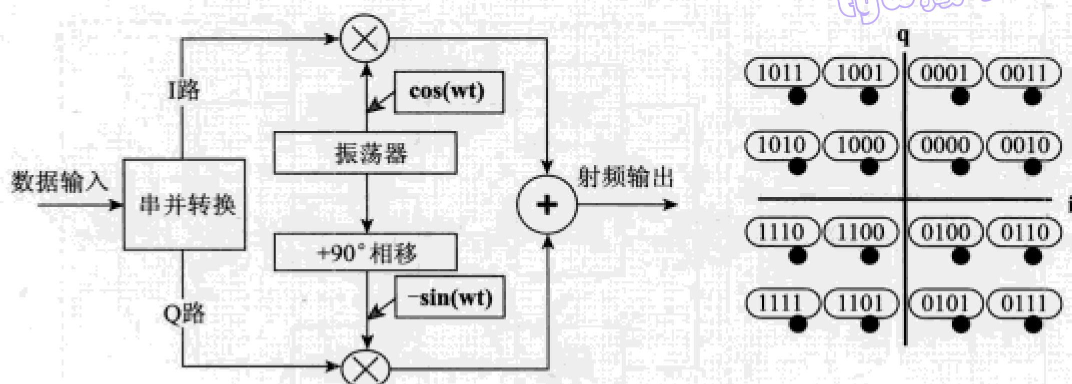


图 5.8 QAM 调制的基本过程及 16QAM 比特星座图

与 R4 的数据能力相比，QAM 的频谱效率以及 AMC 使 WCDMA 的下行比特速率提高了几个数量级。QAM 的调制级数可以达到 64QAM，不过综合考虑到成本、复杂性和效率等因素，对 UTRAN/HSDPA 应用来说，16QAM 是比较合理的。

这样，如图 5.9 所示，WCDMA 使用了两种不同的 QPSK，下行是传统的 QPSK，上行是双 QPSK，下行高速率应用还使用了 QAM。

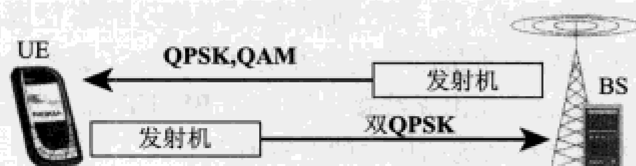


图 5.9 UTRAN 使用的调制方式及其链路方向

5.2.3 接收机技术

WCDMA 充分利用了多径传播的特征，所谓多径传播就是说，发射机发送的信号会经由很多条路径到达接收机。为了提高无线网络的容量，UE 或 BS 应当保持较小的发射功率，以减小无线接口的干扰，为其他传输留出余地。于是，无论是 UE 还是 BS，若能收集携带相同信息的多个弱信号再把它们合并在一起，那将是非常有用的。这样做需要有专门的接收机，一种具体的实例就是 RAKE 接收机（注意 RAKE 不是缩写词，它就是接收机的实际名称）。

信号通过不同路径传输时衰落强度是不一样的，RAKE 接收机的目的就是利用这种多径传播特性来提高信号电平。如图 5.10 所示，RAKE 接收机的基本结构包括多个分支接收机、一个合并器、一个匹配滤波器以及延迟均衡器。每个分支接收机都能接收到一部分发送的信号，这些信号可能来自服务基站或邻基站。不同支路接收到的信号在合并在一起时，合并方式能补偿各路信号在相位和强度上的差别，使合并后信号的强度显著高于任一个分支的信号强度。分支接收机之间必然有一些给定范围的延迟，这是为了让支路能区分出不同的多径信号。

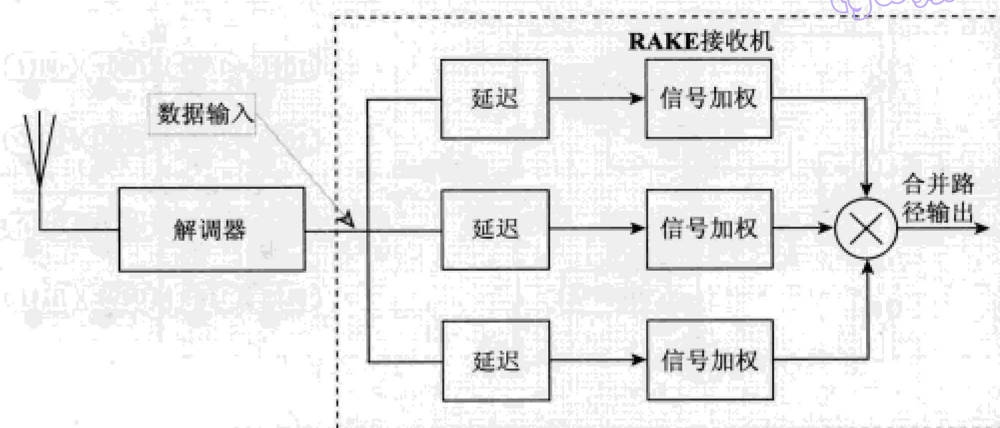


图 5.10 RAKE 接收机的基本原理

一般来说,分集技术能有效抑制无线信号中由阴影和衰落而引起的失真(见第3章)。另外,蜂窝系统中软切换也必然要用到分集技术。移动通信中有许多不同的分集技术,如时间分集、空间分集和频率分集等。WCDMA 在上行和下行传输中都使用了极化分集技术。多径分集技术分辨出多条路径的信号分量,合并后形成质量更好的信号。在 UE 和 BS 端都使用 BAKE 接收机捕获有用信号的多径成分,经合并后可使最终信号或者数据流有更好的质量以便进一步处理。MRC(最大比合并)是信号处理中使用的分集算法。分集的功能由无线接入网中的 BS、UE 和 RNC 承担,具体由传输方向(上行/下行)以及网元在系统结构中的位置有关。

5.2.4 小区容量

在 WCDMA 技术中,所有的用户共享频带为 5MHz 的公共物理资源。WCDMA 中所有用户的收发器(TRX)同时共存于这个频带内,不同的通信靠所使用的扩频码来识别。在第一代 UMTS 系统中,UTRAN 采用 WCDMA-FDD 版本。该版本用不同的频率分隔 Uu 接口上不同的传输方向。最重要、同时也最不明确的问题是 WCDMATRX 的容量。GSM 网络中确定 TRX 容量非常简单,但 WCDMA 无线接口的处理方式完全不同,限制容量的因素也很多,所以 WCDMA TRX 的容量不易确定。

下面简要介绍一定无线环境下 WCDMA TRX 容量的理论估算问题。为简单起见,我们做如下假设。

- 用户在 TRX 覆盖范围内均匀分布,它们到 TRX 天线的距离相同。
- 用户的功率级别相同,因此它们所引起的干扰也在同一水平上。
- TRX 范围内的所有用户都有相同的基带比特速率(符号速率相同)。

在以上假设下,引入定义“处理增益”(G_P),它反映整个带宽(B_{RF})与基带比特速率($B_{Information}$)的相当大小关系:

$$G_P = \frac{B_{RF}}{B_{Information}}$$

也可表示为码片速率和数据速率的比值：

$$G_P = \frac{\text{码片速率}}{\text{数据速率}}$$

无论何种定义，其分贝值表示接收机输出信号相对输入的信噪比（S/N）增益。

稍后我们将看到，处理增益实际等于 SF（扩频因子）。注意此处的基带比特速率指经过速率匹配后的速率。速率匹配将用户的原始比特速率调整到一些固定的承载比特速率上，如 30kbit/s、60kbit/s、120kbit/s、240kbit/s、480kbit/s 和 960kbit/s 等。系统的码片速率是常数、3 840 000chip/s。因此，比方说承载比特速率为 30kbit/s，那么扩频因子就是 128：

$$G_P = \frac{38\ 400\ 000}{30\ 000} = 128 = \text{扩频因子}$$

每个信道上信息传输所需要的功率 P 是每比特需要的能量和基带数据速率的乘积：

$$P = E'_b \times \text{基带速率}$$

另外，整个带宽 B_{RF} 上的信道噪声（$N_{Channel}$）可表示为：

$$N_{Channel} = B'_{RF} \times N_0$$

其中 N_0 是噪声的谱密度（W/Hz）。

因此，信噪比可以表示为：

$$S/N = \frac{P}{N_{Channel}} = \frac{E'_b \times \text{基带速率}}{B'_{RF} \times N_0} = \frac{E_b/N_0}{G_P}$$

假设在 TRX 范围内有 X 个用户，那么根据先前的假设，从统计意义上说就会有 $X-1$ 个用户对一个用户产生干扰。这样，信噪比 S/N 表达为数学形式就是：

$$S/N = \frac{P}{P' \times (X-1)} = \frac{1}{X-1}$$

若用户很多（如几十个），上式可以简化为：

$$S/N = \frac{1}{X-1} \approx \frac{1}{X}$$

于是我们可以用下面两种方法来计算信噪比 S/N：

$$\frac{E_b/N_0}{G_P} \approx \frac{1}{X} \quad \text{或者} \quad X \approx \frac{G_P}{E_b/N_0}$$

这些式子是很粗略的，仅用于估算。计算 TRX 容量时“正式”的方法还需要考虑更多的参数。

例：假设小区使用的 $SF = 128$，$E_b/N_0 = 3\text{dB}$，假设基站只有一个 TRX，问同时可以支持多少个用户进行通信？

$$X \approx \frac{G_P}{E_b/N_0} = \frac{128}{3}\text{dB} \approx \frac{128}{2} = 64 \text{ 用户}$$

这个结果只考虑小区内干扰，TRX 理论上能处理的最大用户数将不会超过这个结果。实际中，相邻的小区还会产生小区间干扰。如果假设小区间干扰和小区内干扰一样大，用户数将减半，成为 32（64/2 = 32）。

E_b/N_0 大小是一个关键，它基本是一个常数，根据无线接口承载比特速率的不同，有几个不同的取值。若容量指同时通信的用户数，E_b/N_0 大小对（TRX/小区的容量）有显著的影响。关于 E_b/N_0，需要考虑下面几个要素。

- N_0 在本地是固定不变的，它涉及接收机自身的一些参量。
- E_b 是一个变值，与下列因素有关。
- 处理增益/扩频因子：扩频因子值越大，E_b 越小。
- 基带比特速率越高，E_b 越大。
- UE 和 BS 接收机之间的距离：距离越大，E_b 越大。
- 终端移动速度：移动速度越快，E_b 越大。

上述只是对 TRX 容量的粗略估算，还有很多其他方法。详见 Holma 和 Toskala 在 2001 年所著的 *WCDMA for UMTS* 一书。

5.2.5 基站中的控制功能

尽管基站的主要功能涉及无线信号的发射接收以及与基带相关的处理功能，基站还具有相关的 UTRAN 控制功能。有些功能是为了无线测量的实施、数据采集和过滤，这些测量结果将提供给 RNC 以执行 RAN 的控制功能。还有一些核心的基站功能，包括码的产生、功率控制和运维，特别是网元级或小区级的运维。基站中的运维功能包括由 RNC 控制的网元级（HW&SW）和 UTRAN 级逻辑功能。主要的网元级功能与具体实现有关，它形成了 NMS（网管系统）的基础。该功能的实现方式取决于厂家。

从无线资源管理的角度看，基站包括内环功率控制和码的产生，新近出现的 R5 增强版也包括了分组调度。因此，UTRAN 的演进也增加了基站的控制功能。不过在 UTRAN 总体控制方面，RNC 仍然处在核心地位。由于目前该技术（尤其与 RRM 联合）正在成为现实，我们将结合其他 RNC 功能进一步介绍这些功能。

5.3 无线网络控制器（RNC）

RNC（Radio Network Controller，无线网络控制器）是 UTRAN 的交换和控制单元，RNC 位于 Iub 和 Iu 接口之间。它也可能有第三个接口称为 Iur，用于 RNS 间的连接。RNC 的实现由厂商决定，但可以概括出一些一般性要点，如图 5.11 所示。

如前所述，RNC 把 BS 看成两个实体：公共传输及节点 B 通信报文集合。对 BS 来说，控制这些的 RNC 称为 CRNC（Controlling RNC，控制 RNC）。

在承载方面，RNC 是 Iu 承载和 RB 之间的交换点，在 UE 和 RNC 之间携带用户数据的无线连接是一个 RB。RB 又与 UE 报文相关。UE 报文是 Iub 要求的一系列定义，用来安排在 UE 和 RNC 之间的公共和专用连接。由于 UTRAN 利用了宏分集技术，因此 UE 和 RNC 之间可能会同时存在多个 RB。这种情形就是稍后要讨论的软切换。对于某个 UE，拥有其 Iu 承载的 RNC 称为 SRNC（服务 RNC）。

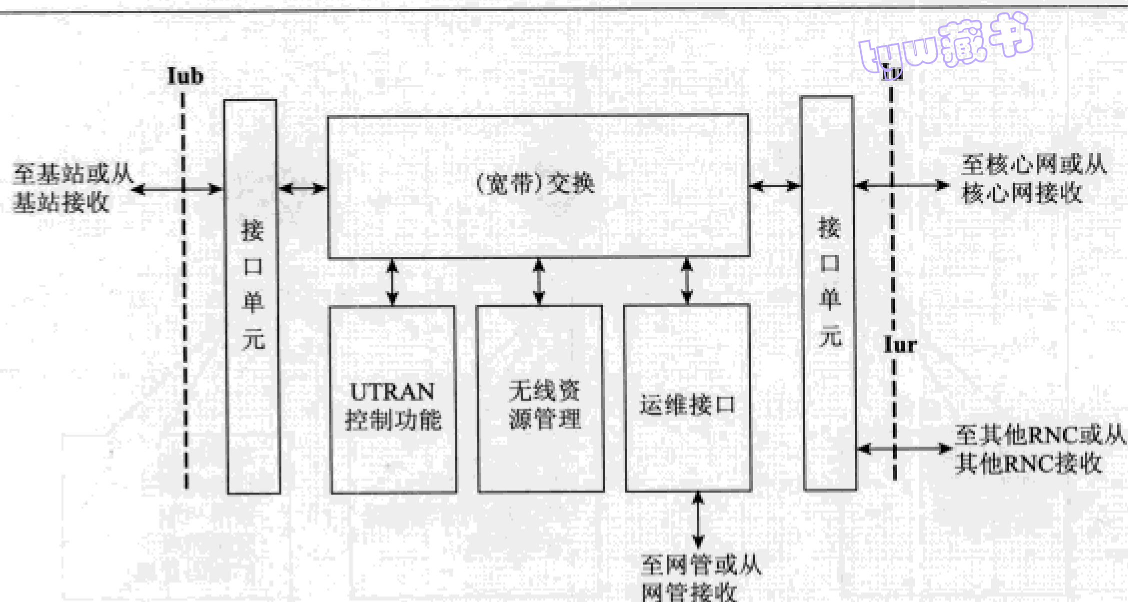


图 5.11 RNC 的基本逻辑结构

RNC 的第三个逻辑功能是 DRNC(Drifting RNC,漂移 RNC)。在此模式下,RNC 把 UE 报文分配到自身,这样的请求通过 Iur 接口来自于 SRNC。

SRNC 和 DRNC 是一些功能角色,其物理位置是可变的。当 UE 在网络中移动并执行软切换操作时,UE 的无线链接将会接到与起初建立 RAB 的 SRNC 完成不同的其他 RNC。此时,SRNC 的功能将转移到这个 RNC 中,由它负责处理 UE 的无线连接。这一过程称为 SRNC 或者 SRNS 重定位。

RNC 的整个功能可以分为两部分:RRM(Radio Resource Management,UTRAN 无线资源管理)和控制功能。RRM 是一系列算法的集合,它通过对无线资源的有效管理和共享,保障无线通道的稳定性和无线连接的 QoS。UTRAN 控制功能包含了所有跟 RB 建立、保持和释放相关的功能,也包括 RRM 算法的支持功能。

5.3.1 RRM

正如第 1 章所述,RRM(无线资源管理)是 UTRAN 中一种管理功能。RRM 位于 UTRAN 中的 UE、BS 和 RNC 之间。RRM 利用各种算法来保障无线通道的稳定性,从而保障无线通道上的业务满足 QoS 要求,如图 5.12 所示。

RRM 算法需要在无线通道上传输信息,这些信息称为 UTRA 业务。它采用 RRC(无线资源控制)协议。本章稍后将讨论 UTRAN 控制功能。RRC 协议在第 10 章介绍。

下面将要介绍的 RRM 算法主要包括以下几项。

- 切换控制。
- 功率控制。
- AC(接纳控制)和 RS(分组调度)。
- 码管理。

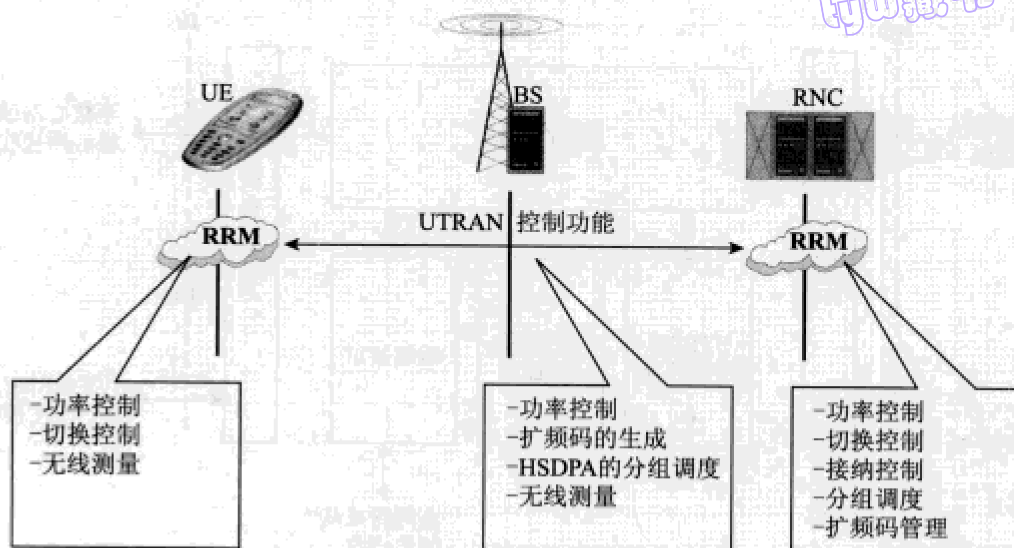


图5.12　无线资源管理的主要实体

5.3.1.1　RRM——切换控制

在移动通信系统中，切换是保障用户移动性的基本方法之一。它使移动中的用户能保持业务连接。切换的概念很简单：当用户从一个小区的覆盖范围移动到另外一个小区的覆盖范围时，在新小区中建立一个新的连接，然后释放和原小区的连接。不过，蜂窝系统中切换控制机制非常复杂，特别是在CDMA（码分多址）系统中还会带来一些更复杂的因素。

5.3.1.1.1　切换的原因

有许多原因会激活切换过程。最基本的原因是空中接口连接已经不能达到预定的准则，为此，UE或者UTRAN将启动一些动作来提高连接的质量。在WCDMA中，电路交换的呼叫在呼叫进程中进行，而分组交换呼叫的切换等到网络或者UE都没有分组在传输时进行。

不论是哪一种切换类型，有个共同点就是现行连接的QoS不可接受而且也不可能优化。还有一个共同点就是如何判断是否需要切换。切换执行准则主要取决于系统使用的切换策略。不过大多数的切换过程的准则都是基于信号质量、用户移动性、业务分布和带宽等因素的。

基于信号质量的切换发生在无线信号的质量或者信号强度低于RNC中规定的某个参数时。信号的恶化是通过UE和BS持续进行的信号测量来检测的。上行及下行链路都可采用基于信号质量的切换。

基于业务的切换发生在小区的业务容量接近最大容量时。此时，小区边缘的高负荷UE可能会被切换到负载较轻的邻小区中。这种切换能使系统负载分布得更为均匀，从而能自动调整所需的容量和覆盖范围以满足网络中的业务要求。基于业务的切换可以通过优先级或者转移重试实现。

切换的次数直接取决于 UE 的移动性。若假设 UE 沿同一方向持续运动,则可认为,UE 移动的越快,UTRAN 所需要的切换次数就越多。为了减少不必要的切换,高移动性的 UE 可能会从微小区切换到宏小区。相反,如果 UE 的移动速度很慢或根本不移动,可能会从宏小区切换到微小区,以提高无线信号的强度同时节省 UE 的电池消耗。

除了业务切换外,是否执行切换都是由服务当前用户的 RNC 决定的。对于业务切换,MSC(Mobile Service Switching Centre,移动业务交换中心)也可能做决定。除上所述外,还有许多其他的原因需要进行切换,例如业务的改变。

5.3.1.1.2 切换过程

图 5.13 示出的基本切换过程包括三个阶段:测量阶段、决定阶段和执行阶段。我们这里讨论整个切换过程是针对 WCDMA 而言的,但其基本原理对任何蜂窝系统都是适用的。

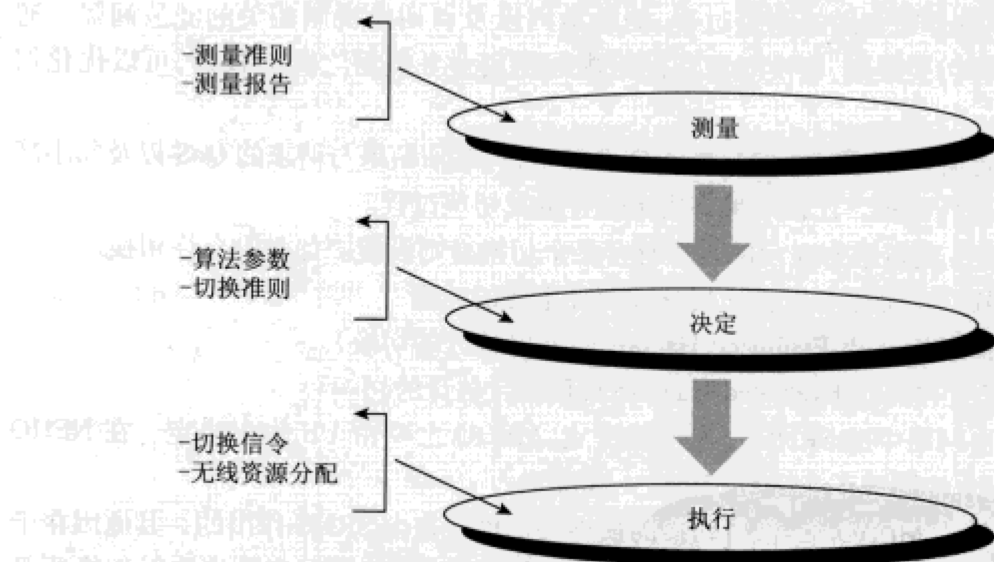


图 5.13 切换的基本过程

切换测量从系统性能的角度来看是一个非常关键的功能。首先,小区环境和用户移动性引起的衰落和路径损耗可能导致无线信号强度的急剧变化。其次,过度的 UE 测量报告或切换会在总体上增加网络信令,这是不期望出现的。

在 WCDMA 中,为了实现切换功能,UE 在业务连接过程中连续测量邻小区的信号强度,并报告给网络。

根据 3GPPTS25.331,UE 应做的测量分成这样一些不同的类型。

- 同频测量,对同一频率,测量下行物理信道上的信号强度。
- 频率间测量,对不同频率,测量下行物理信道上的信号强度。
- 系统间的测量,对 UTRAN 以外的接入系统(如 GSM),测量下行物理信道上的信号强度。
- 业务量测量,测量上行业务量。

- 质量测量,测量质量参数,例如下行传输块错误率。
- 内部测量,测量 UE 的发射功率和接收电平。

另外,下列事件也会触发测量。

- 最佳小区改变。
- CPICH(主公共导频信道)信号电平改变。
- P-CCPCH 信号电平改变。
- 信噪比(SIR)改变。
- 干扰信号码的功率改变。
- 周期报告。
- 定时触发。

因此,WCDMA 标准提供了多种测量准则来支持系统中的切换机制。为了提高系统性能,必须选择最合适的测量过程、测量准则以及和切换机制相关的滤波间隔。通过仔细地进行切换准则、切换测量和网络规划所用业务模型之间的权衡,可以优化切换信令负荷。

切换决定阶段包括对连接的整体 QoS 评估,将评估结果与请求的 QoS 以及邻小区的估计结果进行比较。比较结果将决定是否触发切换过程。

SRNC 检查测量报告显示的是否符合某个切换准则设置。如是则允许切换。

根据切换判决准则可以把切换分成两种主要的类型。

- NEHO(Network Evaluated Handover,网络估计的切换)。
- MEHO(Mobile Evaluated Handover,移动台估计的切换)。

NEHO 由网络中的 SRNC 作出切换决定,MEHO 主要由 UE 作出决定。在 NEHO 和 MEHO 组合的情况下,UE 和 SRNC 一起决定。

注意即使在 MEHO 中,执行切换的最终决定也还是由 SRNC 作出的。其原因在于 RNC 整体负责系统的 RRM 功能,所以它清楚系统总的负载情况和其他执行切换所必需的信息。

切换决定基于 UE 和 BS 的测量报告以及切换算法所设置的准则。切换算法不受标准约束,可以独立实现。因此,根据网元的测量能力、业务分布、网络规则、网络结构和运营商的整体业务策略等,可以自由选用更先进的切换算法。

切换算法的一般原理如图 5.14 所示。此例假设算法的决策准则基于 UE 报告的导频信号强度,其中用到了以下术语和参数。

- 上门限:对于一定的 QoS 要求,最大可接受的信号强度。
- 下门限:对于一定的 QoS 要求,最小可接受的信号强度。信号强度不应低于此值。
- 切换余量:是一个预先设定的参数,指这样一个点,从此处开始,邻小区(B)信号强度比本小区(A)大;或者到此处时,邻小区信号强度已经持续一段时间比本小区好。
- 激活集:指 UE 同时连接到 UTRAN 的信号支路(小区)的集合。

假定一个 UE 在小区 A 中驻留并向小区 B 移动。随着 UE 向小区 B 靠近，UE 目前连接的导频信号恶化，逐步接近图 5.14 所示的下门限。这就可能导致切换的触发，其过程可分为下面几个步骤。

①信号 A 的强度和定义的下门限相等。同时，RNC 根据 UE 的测量结果得知，存在一个有足够强度的邻近信号（图 5.14 中信号 B）可用于提高连接质量。因此，它把信号 B 加入到激活集。此时，UE 同时有两个到 UTRAN 的连接，利用信号 A 和信号 B 构成的和信号就可以改善连接质量。

②在这一点，信号 B 的质量开始比信号 A 要好。因此 RNC 以这一点作为计算切换余量的起始点。

③信号 B 的强度开始好于预定的下门限。其强度足以满足所需要的 QoS。另一方面，和信号的强度超过了预定的上门限，将增加系统中的干扰。于是，RNC 从激活集中删除信号 A。

激活集的大小是可变的，一般包含 1 ~ 3 个信号。在上述这个例子中，在步骤① ~ 步骤③期间激活集的大小为 2。

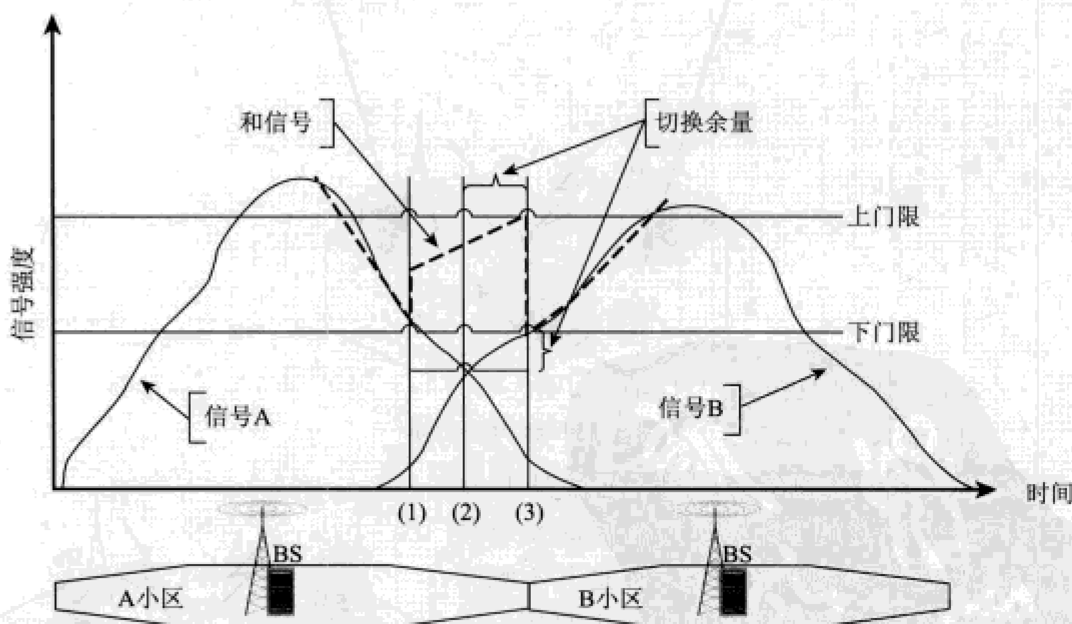


图 5.14　切换算法的基本原理

UE 的移动方向在随机改变，因此有可能在切换之后又迅速回到小区 A。这就是所谓的乒乓效应，对系统的容量和总体性能来说是一个不利因素。这种不期望的切换会增加 UTRAN 的信令负荷，避免它的最好方法就是采用切换余量或滞后参数。

5.3.1.1.3　切换类型

根据切换机制中的分集情况，可以把切换分成三类：硬切换、软切换和更软切换。硬切换可以进一步分为频内切换和频间切换两种。UMTS 系统支持所有这些切换类型。

在切换过程中,如果在建立新连接之前释放了旧的连接,称为"硬切换"。因此在硬切换过程中,UE 不仅不可能同时和多个基站连接,还会有一段时间非常短的、移动用户不能觉察的中断。

在频间硬切换中,UE 新无线接入的载频和原来的载频不同。换言之,如果切换后UE 接入所用的载波和原先相同就是频内切换。

图 5.15 和图 5.16 示出了邻基站分别用同频和异频发送的硬切换情形。

在图 5.15 中,由于无线网络规划策略或者传输等原因,相邻的两个 RNC 并没有和 Iur 接口相连,因此 RNC 间的软切换是不可能的。在这种情形下,能支持用户从原基站到新基站之间的移动性及无缝无线接入的唯一选择就是频内硬切换。这也会导致 RNC 间的切换事件,并会涉及 MSC。

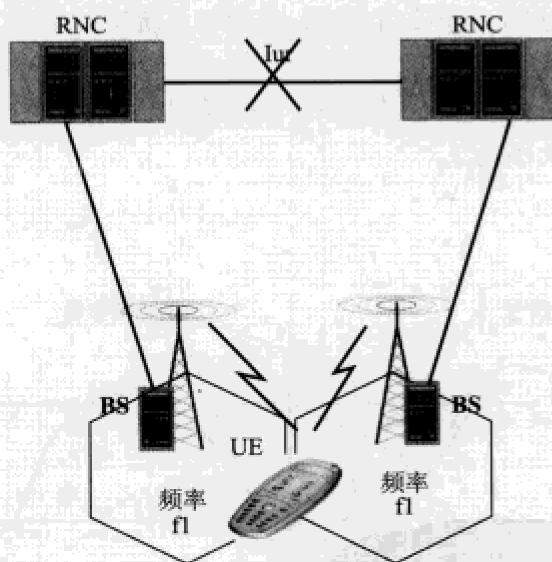


图 5.15 频内硬切换

WCDMA 系统的频率复用因子通常是 1,也就是说网络中所有的 BS 都使用相同的发射频率,所有 UE 也共享相同的频率。但这并不意味着 WCDMA 系统不能使用其他的频率复用。因此,如果出于其他原因,不同的小区使用了不同的载频,就需要采用频间切换使得小簇中的邻小区之间有一个切换路径。

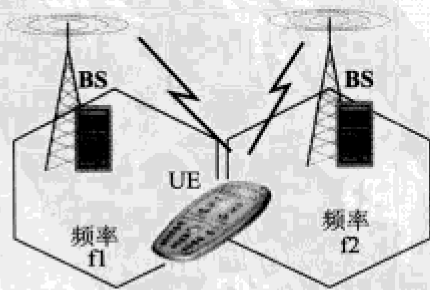


图 5.16 频间硬切换

在采用 HCS(Hierarchical Cell Structure,分级小区结构)的网络中,频间切换也会发生在使用不同频率覆盖相同范围的不同层之间,例如在宏小区和微小区之间。此时,频间切换不仅是为了保证 UE 的连接不中断,也是为了提高系统在容量和 QoS 方面的性能。频间硬切换总是由 NEHO(网络决定的切换)。

另外,频间切换也可能发生在两个不同的RAN(Radio Access Network,无线接入网络)之间,例如发生在GSM和WCDMA之间。这种情形下的切换也可以称之为系统间切换(见图5.17)。系统间切换总是频间切换,因为不同的系统所使用的频率不同。

WCDMA系统中的一种特殊功能模式——压缩模式(或称时隙模式)可用来实现系统间切换。从WCDMA的角度来看,当UE处于时隙模式时,信道的扩频因子值可以减少。其结果是无线连接只占用了WCDMA帧中的一部分时间,余下来的时隙可用于其他目的,例如UE可在这些时隙中测量周边的GSM小区。换言之,这种方法可以实现UTRAN所要求的GSM/UMTS互操作性。实现时隙模式的方法可以通过高层控制来减少数据速率,或者通过物理层复用来降低符号速率。当UE以这种模式使用Uu接口时,WCDMA的帧就被压缩以开出一个时间窗口,通过该时间窗口,UE就可以识别和解码GSM的BCCH(Broadcast Control Channel,广播控制信道)。另外,WCDMA RAN和GSM BSS(Base Station System,基站系统)都必须通过BCCH发送彼此的识别信息,以使UE能正确解码。

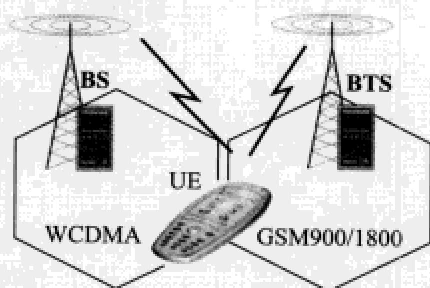


图5.17 系统间切换

WCDMA和GSM间的系统切换可用于WCDMA和GSM共存的环境中。为了保证业务的连续性,需要通过系统间切换来互补覆盖范围。当WCDMA和GSM两个系统的覆盖互相重叠时,也可以通过系统间切换来控制GSM和WCDMA系统之间的负载。其他可导致系统间切换的因素包括UE的业务请求和用户的业务定制。

系统间切换是网络发起的切换,UE应能完全支持系统间切换。RNC根据无线网络中邻小区的配置以及其他控制参数来判断是否可以进行系统间切换。GSM RAN中的BSC也如此。

和硬切换不同,软切换在原连接释放之前就建立了新的连接。WCDMA系统中绝大多数的切换是频内软切换。如图5.18所示,参与软切换的相邻基站用相同的频率发送。

软切换是在不同基站的两个小区间进行,这两个基站不一定属于同一RNC。参与软切换的RNC应通过Iur相互协调软切换的进行。在软切换中,源小区和目的小区使用相同的频率。对于电路交换的呼叫,如果无线网络环境的小区很小,终端几乎总处在软切换中。软切换有几种不同的类型,包括更软切换和软－更软切换。

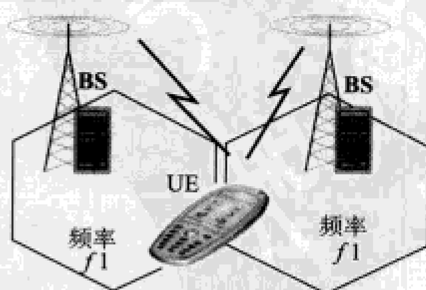


图5.18 频内软切换

在更软切换中,激活集中新增一个信号、或者

删除一个信号、或者用一个更强的信号替换旧信号，该更强的信号在同一个基站控制的不同扇区中，如图5.19所示。

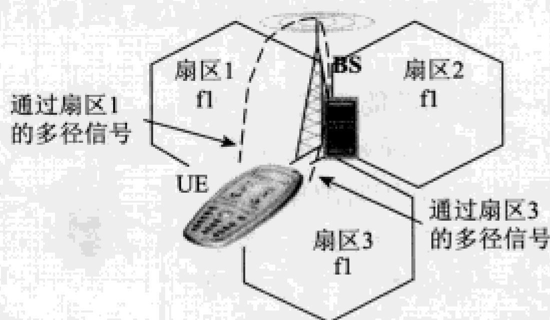


图5.19 频内更软切换

在更软切换过程中，BS 通过一个扇区进行发送，但接收是通过多个扇区进行的。此时 UE 通过同一 BS 内的多个扇区同时建立多个激活的上行无线连接。

同时发生软切换和更软切换的情形称为软－更软切换。发生软－更软切换的情形比如是，在 RNC 间切换时，UE 在激活集中加入了一个邻扇信号的同时，又加入了一个来自其他 RNC 所控制小区的信号。

讨论软切换和激活集时，在处理多径分量方面有两个术语：微分集和宏分集。

微分集是指多径传播分量在 BS 端进行合并，如图5.20所示。WCDMA 利用多径传播。就是说基站端的 RAKE 接收机（见5.2.3节的介绍）能够识别、区分出无线信道上的多个信号，并将它们合并在一起。在实际系统中，无线信道中的发送信号经地面、水面和建筑物等的反射后，接收机端可以接收到原始信号的多个副本，它们到达接收机时的相位和时间有少许不同。BS 级的微分集功能将同一个小区中接收到的多径信号合并在一起，如果多径信号来自多个扇区，就称为更软切换。

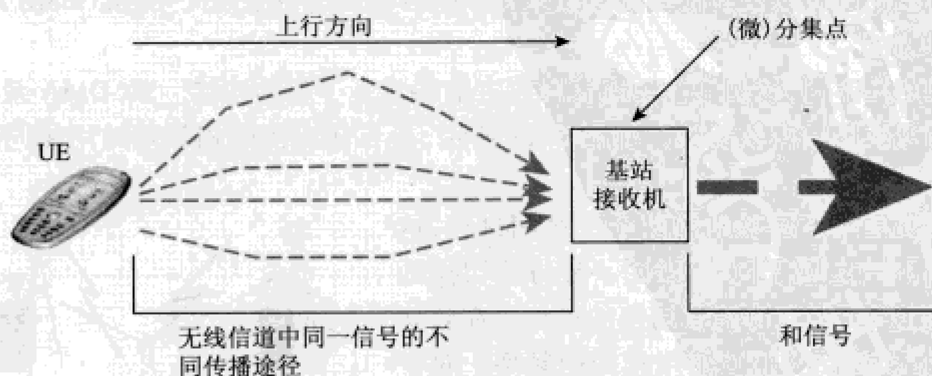


图5.20 基站中的微分集

由于 UE 可以使用不同 BS，甚至不同 RNC 下的小区，因此就有了 RNC 级的宏分集功能。不过其合并方法与基站中的微分集有很大的不同，因为 RNC 没有 RAKE 接收机。因此，RNC 利用数据流的质量等其他方法来合并或者选择所需要的数据流。在

图5.21示出的例子中,UE的激活集包括3个小区,其中一个与另一个RNC相连。BS首先将它自己的无线信道上的信号进行合并,数据流的合并在RNC这一级进行。

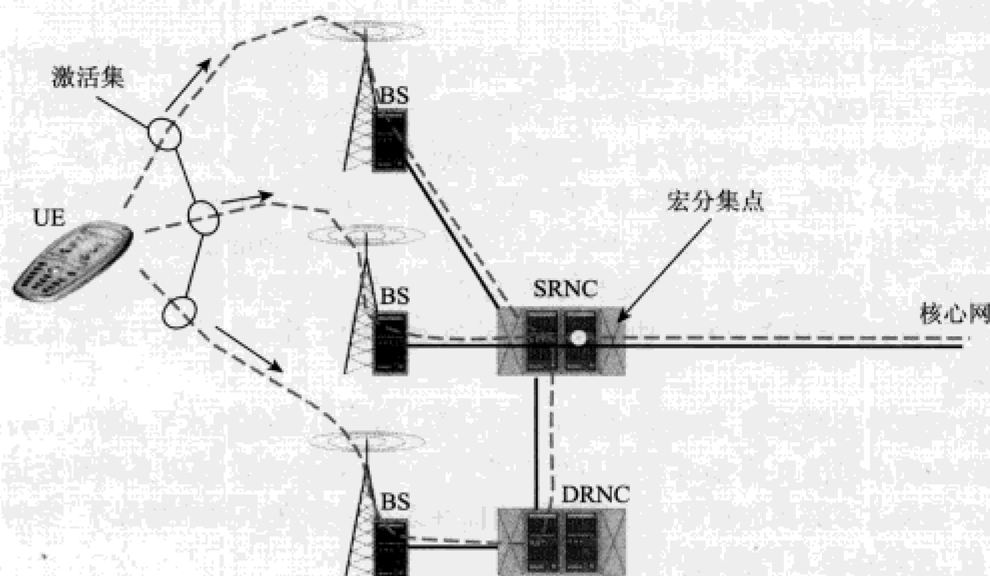


图5.21 RNC中的宏分集

软切换和更软切换的想法是,多个来源(多径传播)的信号所合并的"最终"信号有更好的主观话音质量。在GSM系统中,主观话音质量与发射功率有关,大致来说,发射功率越大,信号质量越好。而在WCDMA中,终端不能随便增加发射功率,因为太大的发射功率会阻塞其他的用户。因此更好的方法是利用多径传播来提高主观呼叫质量。

总而言之,软切换和更软切换会消耗无线接入容量,因为UE在Uu接口上占了不止一条无线链路连接。但从另一方面来说,如果运用得当的话,软切换和更软切换由于减小了干扰而增加的容量更大,整体上还是增大了系统的容量。另外值得一提的是,更软切换能更好地利用传输网络的容量,它只在BS级进行合并,没有用宏分集,不仅有能利用多径传播的优点,同时还能最小化传输资源。因此,WCDMA的BS站址增容首先就是扇区化。不能再增加扇区时,就采用新频率的载波。

从系统结构的角度来看,UMTS网络支持以下几种类型的切换。

- BS内/小区间的切换(更软切换)。
- BS间切换,包括硬切换和软切换。
- RNC间切换,包括硬、软和软-更软切换。
- MSC间切换。
- SGSN(GPRS业务支持节点)间切换。
- 系统间切换。

5.3.1.2 RRM——功率控制

功率控制是任何基于CDMA的蜂窝系统的一个基本特征。不使用精确的功率控

制机制，这些系统就不能工作。在下面几节中，我们首先说明为什么功率控制对这些蜂窝系统是必须的，并且介绍其中的一些主要因素，然后介绍 WCDMA-FDD 无线接入系统所用的功率控制机制类型。

近效应、WCDMA 中干扰受限的容量，以及 UE 有限的能量资源是采用功率控制的主要原因。与 FDMA(Frequency Division Multiple Access，频分多址)以及 TDMA(Time Division Multiple Access，时分多址)等带宽受限的多址方式不同，WCDMA 是一种干扰受限的多址接入方式。在 FDMA 和 TDMA 中，功率控制是为了减少蜂窝系统中因频率复用而产生的小区间干扰，但在 WCDMA 系统中，功率控制的主要目的在于减少小区内的干扰。为此需要优化无线发射功率，即把每个发射机的功率调到满足 QoS 要求的水平。不过，确定这样的发射功率是一个非常复杂的工作，原因在于无线信道是动态变化的。

无论是何种无线环境，接收机收到的功率都应达到可接收的水平，例如上行链路基站收到的功率应能支持 QoS 要求。功率控制的目标就是将发射功率调到合适的水平，UE 不用发送不必要的功率。这样就能确保在系统内存在干扰的情况下，发射功率不高不低，正好在要求的范围内。

多径传播特性以及 WCDMA 系统的技术特征(同频带被多个用户同时共享和远近效应)，使得功率控制成为 WCDMA 系统的必备技术，以克服无线环境和电波特性带来的问题。如果没有功率控制，那么衰落和干扰等现象会使系统稳定性降低，最终使性能急剧恶化。

无论是先进蜂窝技术的提供商，还是蜂窝网的运营商，最大化系统容量都是最终的追求目标。如果系统中的每个终端的发射功率都能够控制到使得到达 BS 的信号能满足最小的信噪比需求，那么就可以保证系统容量最大化。如果一个终端的信号到达 BS 时功率太低，那么无线连接的 QoS 要求就不能得到满足；如果基站端接收到的信号功率太大，尽管该终端的性能非常好，但它会对系统中其他的移动台造成巨大干扰，使得其他 UE 的性能恶化，从而造成系统容量的降低。

由于在 WCDMA 系统中总带宽是同时共享的，对某个特定用户来说，系统中的其他用户如同噪声一样的干扰。如果没有功率控制机制或者工作不良，这样的带宽共享就会产生很大的问题，这种问题一般称为远近效应。在远近效应中，离服务基站近的终端的信号会压过离基站远的终端的信号，如图5.22所示。产生远近效应的主要因素包括用户离开基站距离不同引起的路径损耗不同、衰落引起的变化，以及电波传播机制造成的信号功率变化等(见第3章)。

在 WCDMA 系统中，消除远近效应的措施包括功率控制、分集技术、软切换、多用户接收机技术，以及更一般的能抵抗远近效应的接收机。由于远近效应对 WCDMA 系统的性能有严重影响，所以功率控制机制最重要的目的就在于消除远近效应。功率控制对 WCDMA 系统容量有很大的影响。

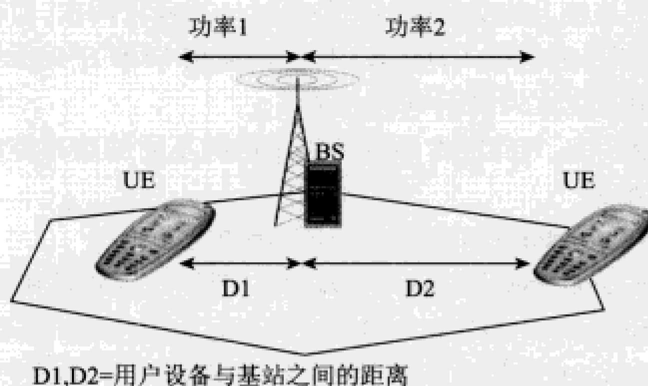


图 5.22 CDMA 系统中的远近效应

5.3.1.2.1 功率控制的基本方法

根据前面的讨论容易看出,上行链路最佳的情形是,无论每个 UE 到基站的距离是多少,到达基站的所有 UE 的接收功率相等。这时的信噪比是最优的,BS 接收机能够解码出最多数量的传输信号。不过在实际中,无线链路是特别不稳定的,并且不同用户的业务要求也不同,甚至同一个用户在同一无线连接中业务也会变化。因此,必须要有一个高效的机制来准确控制每个 UE 的发射功率。

为此,人们对功率控制问题进行了深入的研究,自 CDMA 出现以来,已经提出了许多功率控制算法,包括分布式、集中式、同步、异步、迭代式和非迭代式等许多不同的类型。目前的大多数算法都以 SIR(信噪比)或者发送功率作为功率控制决策过程的参考值。

CPC(Centralised Power Control,集中式功率控制)的主要原理是把所有的功率控制机制集中进行。这种功率控制算法需要有一个中央控制器,它需要已知 RAN 中所有无线连接的信息。

与 CPC 技术不同,分布式功率控制技术不需要采用中央控制器。它把功率控制算法分布在整个 RAN 中。这使其特别具有吸引力 。CPC 技术的主要问题是会增加复杂性、延迟和网络的脆弱性,分布式功率控制的主要优点是更能适应可变的 QoS,这对 WCDA 这种有分组传输的蜂窝系统来说尤为重要。

5.3.1.2.2 UTRAN(WCDMA-FDD)中的功率控制机制

WCDMA 的上、下行都有功率控制。下行功率控制的主要目的是降低对其他小区的干扰,抵挡来自其他小区的干扰并获得可接受的 SIR 值。虽说功率控制对于下行并不如对于上行那么重要,但因为控制小区间干扰能改善系统性能,所以下行也实现了功率控制。

上行功率控制的主要目标是通过使相同 QoS 要求的用户在基站处接收到尽量相同的功率来克服远近效应。因此上行功率控制用来细调终端的发射功率以有效减少小区内干扰和远近效应。注意 WCDMA 标准中的功率控制技术从原理上说是分布式的。

GSM 中的功率控制技术明显不适用于 WCDMA,故此 WCDMA 采用了不同的方

法。在 GSM 中，无线连接上的功率控制每秒执行一次或者两次，而在 WCDMA 中，由于其重要性，功率控制每秒执行 1 500 次（功控周期按 DCH 中的无线帧重复）。因此 WCDMA 的功率控制速度大大快于 GSM 系统。

为了良好地控制功率，WCDMA 系统使用了两种不同的功率控制机制，如图 5.23 所示。它们是以下两项。

- OLPC（Open Loop Power Control，开环功率控制）。
- CLPC（Closed Loop Power Control，闭环功率控制），包括内环和外环功率控制机制。

联合使用这些不同的功率控制机制，UTRAN 通过重叠使用内环闭环功率控制和外环闭环功率控制使目标 SIR 维持在可接受的水平，同样能具有 CPC 技术的优点。

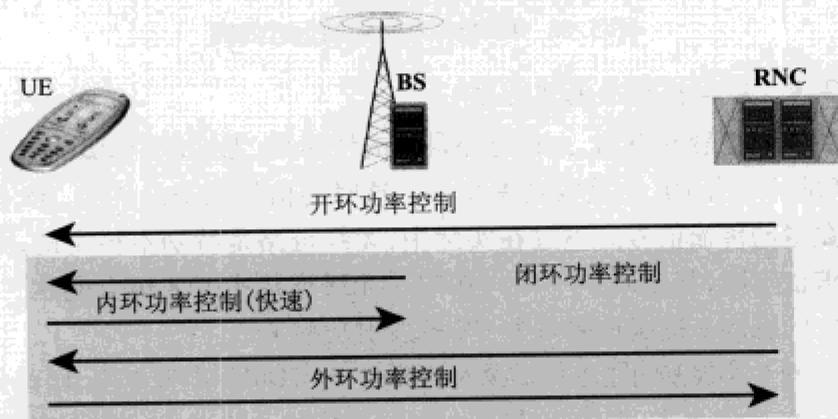


图 5.23　WCDMA 中的主要功率控制机制

5.3.1.2.3　开环功率控制（OLPC）

开环功率控制一般用于上行链路的功率调整。当 UE 处于 Idle 状态，并且还没有发送 PRACH（物理随机接入信道），这时候 UE 根据其接收到的 BS 的 CPICH 信号强度来估计 UE 的初始发射功率。此外，UE 处于 Idle 状态时还从小区的 BCCH 信道中得到各种允许的功率参数信息。然后 UE 估计路径损耗的大小，连同 BCCH 中的数据一起确定初始化连接所需要的发射功率。

图 5.24 示出了上行链路的开环功率控制。UE 测量来自基站的下行导频信号强度来，按照导频信号成反比的方式来估计上行发射功率的大小。也就是说，接收到的导频信号强度越大，UE 的发射功率就越小。

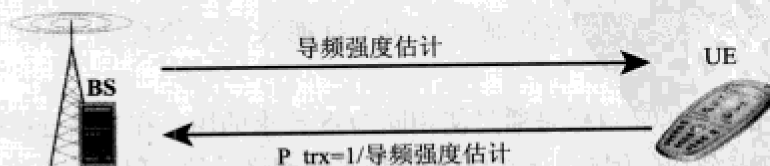


图 5.24　上行开环功率控制

在 WCDMA FDD 中,只采用开环功率控制不足以调制 UE 的发送功率,因为无线信道的衰落特性在上、下行都是快速独立变化的。因此,为了补偿信号强度的快速变化,还需要采用闭环功率控制。不过,开环功率控制对确定初始发射功率、克服对数正态分布的路径损耗和阴影衰落还是很有用的。

5.3.1.2.4 闭环功率控制

CLPC(闭环功率控制)对已经建立的无线连接调整发射功率,其主要目的补偿无线信号强度的快速变化,所以 CLPC 应该足够快以便能跟上信道的快速变化。

图 5.25 示出了 WCDMA 标准中上行闭环功率控制的基本机制。BS 以 1.5kHz(即每秒1 500次)的频率指示 UE 按 1、2 或者 3dB 的步长增加或者减小其发射功率。发射功率应该增加还是减小是根据 BS 估计的接收 SIR 决定的。BS 将接收到的信号同预设的门限值进行比较。如果 UE 的发射功率超过这个门限值,BS 将发送 TPC(Transmission Power Command,传输功率指令)给 UE,要求 UE 降低其信号功率。如果接收到的信号功率低于门限值,BS 将发送指令要求 UE 增加发射功率。需要强调的是,在决定是否控制发射功率时,可以采用多种测量值作为比较接收质量的参数,例如 SIR、信号强度、FER(Frame Error Ratio,帧错误率)和 BER(Bit Error Ratio,误比特速率)等。

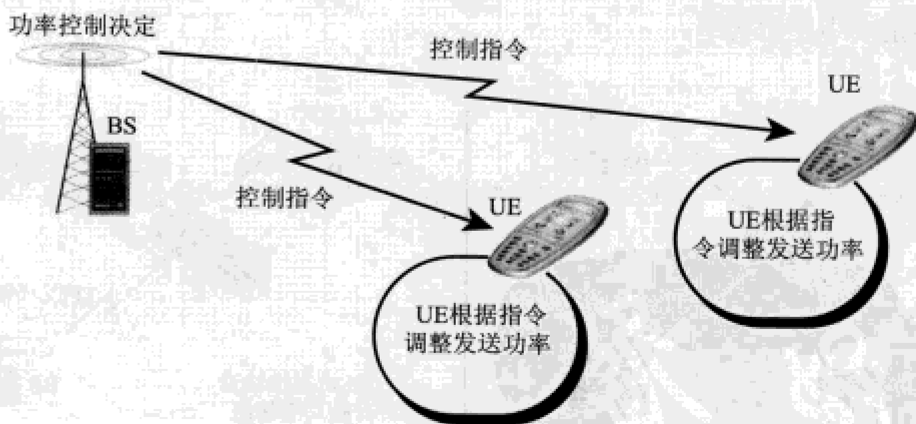


图 5.25 上行链路闭环功率控制的基本机制

下行链路也采用了闭环功率控制来调整发射功率。在下行闭环功率控制中,BS 和 UE 的角色互换,UE 将来自 BS 的信号强度与预设的门限进行比较,然后发送功率控制指令给 BS,BS 根据指令调整下行链路的发射功率。

WCDMA 中的闭环功率控制包括内环和外环两种。前述的闭环功率控制是指内环功率控制,它是 WCDMA 系统中最快速的环路功率控制机制,因此有时也称为"快速功率控制"。

闭环功率控制中的另外一种就是外环功率控制,其主要目的是将上行内环功率控制中的目标 SIR 调节到能使信号质量满意的水平。由于宏分集可以使 RNC 知道目前无线链路连接的条件和质量,因此 RNC 能够确定出小区允许的功率水平以及 BS 计算

功率控制指令时需要的 SIR 目标值。为了保证无线连接的质量,RNC 用这样的功率控制方法来调整目标 SIR 值,从而能保持对无线连接质量变化的核查。这样,网络就能补偿无线接口传播状况的变化,获得最佳的连接质量。实际上,外环功率控制在微调内环功率控制的性能。

总之,对于任何一种蜂窝系统,特别是 CDMA 系统来说,开环和闭环功率控制机制在延长电池寿命和增加系统容量方面有非常重要的作用。

5.3.1.2.5 特定情况下的功率控制

在 WCDMA 中,除了上述这些一般的功率控制机制外,对于一些特殊情况,也有相应的发送功率控制方法。这些情况包括软切换模式、SSDT(Site Selection Diversity,站点选择分集发射)和压缩模式(或者称为时隙模式)等。

在软切换状态下,UE 同时连接到多个基站,因而能收到多个功控指令,UE 通过选择最适当的功率控制指令来调整发射功率,如图 5.26 所示。此时因为 UE 接收到来自不同 BS 的多个 TPC 命令,这些指令的内容可能互不相同。出现这种情况的原因可能是由于功率控制指令没有差错保护,也可能很简单,就是因为无线传输环境不同所致。内容不同的指令使 UE 无可适从。解决这一问题的基本方法是:只要有一个指令要求降低功率,UE 就降低功率。UE 还可以利用门限来检测指令的可靠性,依此决定是应该增加还是减小发射功率。

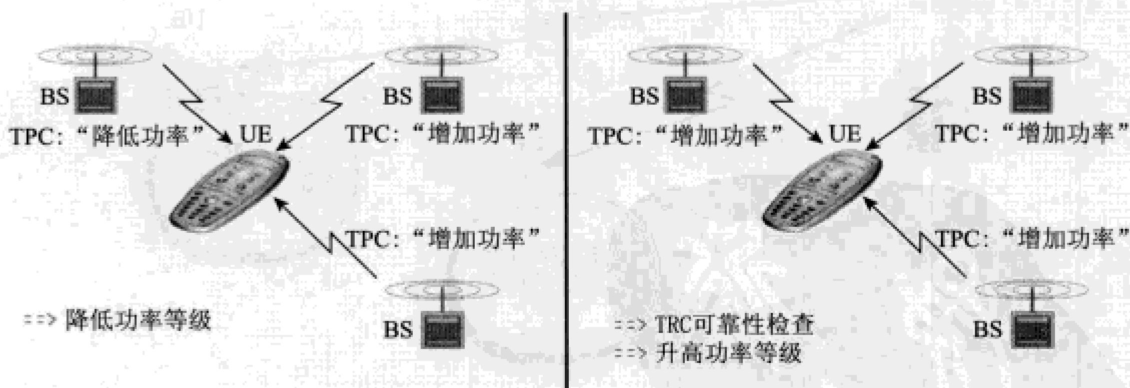


图 5.26 软切换模式下 WCDMA 功率控制的基本原理

SSDT 是功率控制中的另一种特殊情况。SSDT 的原理是:动态选择具有最强信号的基站,只让它发射(见图 5.27),其他和同一 UE 同时连接的 BS 关闭其 DPDCH。因此,UE 根据信号最强基站的指令来调整发送功率。当用户处于软切换模式时,这种方法能降低下行链路上的干扰。

在压缩模式下,BS 和 UE 在预设的时间内停止发送和接收,以便留出时间执行频间无线测量(例如为了系统间切换)。这也使功控操作出现中断。此时功控指令的接收端(如上行的 UE)可采用更大的步长来增加或者降低发射功率,这样就能尽快达到要求的 SIR。

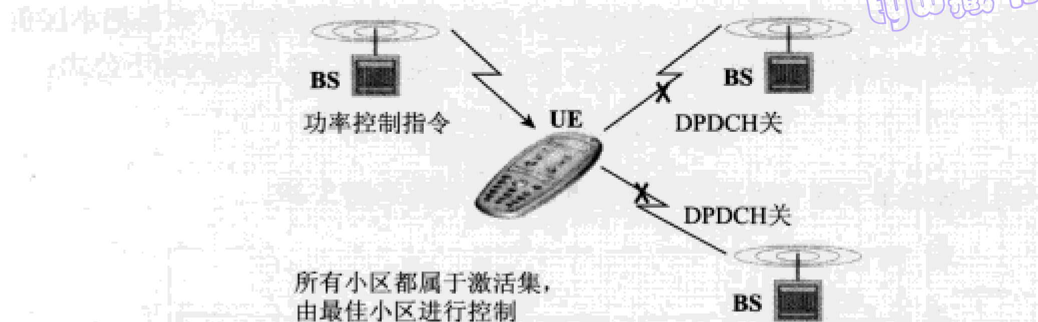


图 5.27 SSDT 技术

5.3.1.3 RRM——接纳控制(AC)和分组调度(PS)

WCDMA 无线接入技术有其自身的限制因素，有系统设计原理方面的，也有环境方面的。最重要的、同时也最困难的是如何控制无线信道特性造成的干扰。WCDMA 中每个 UE 所发射的信号对其他 UE 来说都是一种干扰源。对 WCDMA 蜂窝网络进行规划时，一个基本工作就是确定出网络正常工作可接受的干扰水平。制定出一个能与 UE 实际发送信号相匹配的门限值是非常困难的，也会制约无线接口的容量。

具体而言就是要预先定义一个 SIR 值。理论上说，只要小区内的 SIR 不超过这个值，网络就是稳定的。也就是说，在 BS 接收机中，干扰和信号的功率之间要有一个差额，这样 BS 才能提取出同一载波上的各个信号(码)。如果干挠与信号在功率上差别很小，BS 就不能够从载波中提出单个信号(码)。每一个存在激活连接的 UE 都要“耗用”一部分 SIR，当 BS 接收机无法从载波中提取信号时，这种资源耗费就达到了上限。

AC(Admission Control，接纳控制)的主要任务就是判断接入一个新的呼叫会不会牺牲已有呼叫的业务要求(见图 5.28)。因此，接纳控制算法应能预测出新呼叫接入系统后的小区负载。注意接纳控制算法也要检验地面传输资源是否够用。RNC 根据接纳控制算法准许或者拒绝新呼叫的接入。

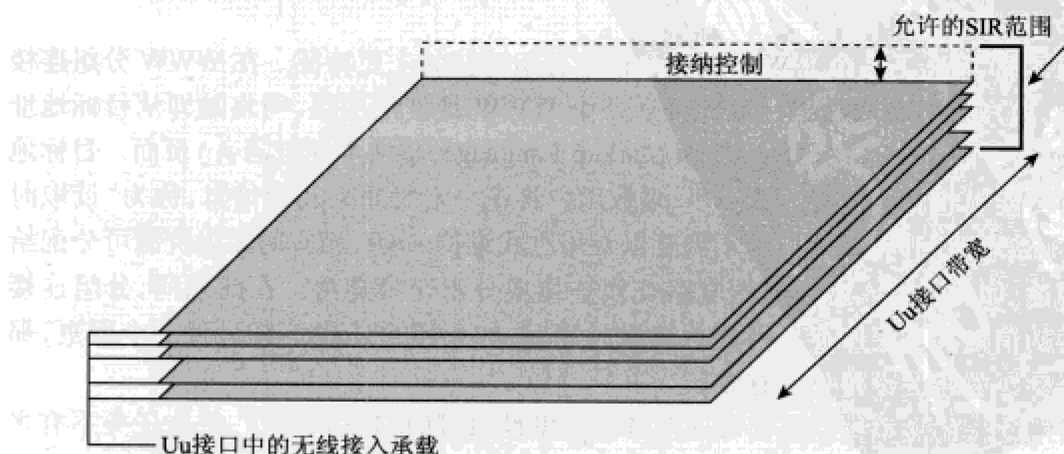


图 5.28 接纳控制的主要原理

从理论上来说，可以把SIR或干扰余量同小区负载直接联系起来。如果把小区负载表示为百分比形式的“负载因子”（见图5.29），记干扰余量为I，可得到如下公式：

$$I = 10 \times \mathrm{Log}\left(\frac{1}{1-\text{负载}}\right)$$

把不同负载因子下的干扰余量计算结果画在一起就是图5.29。

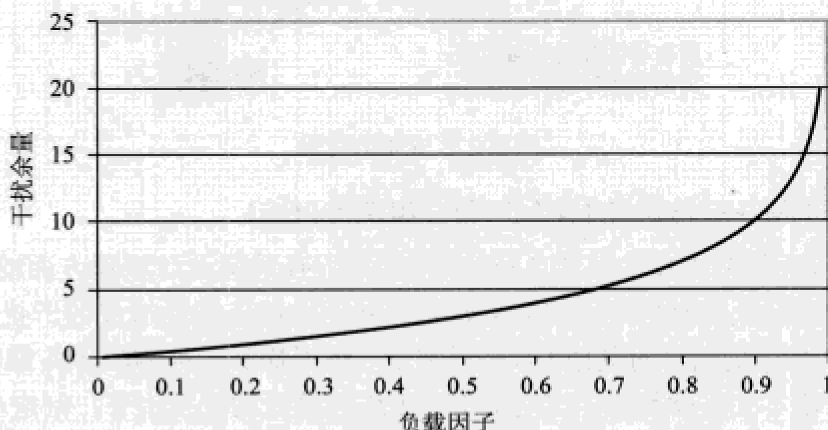


图5.29　干扰余量作为小区负载的函数

从图中容易看出，当小区负载超过70%时，干扰就很难控制了。因此WCDMA网络中，预期容量的等效负载因子设计为50%。这样的设计留有一定的安全余量，能保证系统稳定工作。

在UMTS系统中，业务的特性决定了其既可以是RT（Real Time，实时）的也可以是NRT（Non-Real Time，非实时）的，必须仔细地平衡和控制这些业务。实时业务和非实时业务的控制方法完全不同。主要差别在于，实时业务（电路交换的呼叫）以专用方式连续维持一个RAB，而非实时业务（分组连接）中信道状态随RB比特速率不断变化，系统的负载也跟着变化。因此，分组连接的接纳过程应考虑比特速率可变和突发的特征。

图5.30示出了一个WWW浏览会话中分组连接的主要特征。在WWW分组连接过程中，用户为了获取数据一般先发送一个WWW地址给网络，网络随即从目标地址下载数据，一般是HTML（HyperText Markup Language，超文本标记语言）页面。目标地址也有可能引起文件下载。下一步，多数用户将花一定时间来阅读信息，称为“读取时间”。在读取时间内，接纳控制不需要以专用方式维持RAB，相应的无线资源可分配给其他用途，如其他呼入或呼出的电路交换连接或分组交换连接。在此期间，分组连接会话中的信息在上层保存。因此在读取时间后，如果用户还想下载另外一个网页，那么这个呼叫的相关设置仍然有效。

分组连接的接纳控制需要考虑业务的突发性（即随机到达时间）、每个任务下有多少个分组呼叫，每个呼叫的读取时间和分组的数量。为此，接纳控制必须利用非常复杂的业务模型和统计方法来最佳地控制RAB请求。这可以通过调度非实时业务

RAB,接受、排队和拒绝实时业务 RAB 来实现。维护和控制接受 RAB 的 QoS,控制它们对 UTRAN 整体性能的都在接纳控制的范围内。

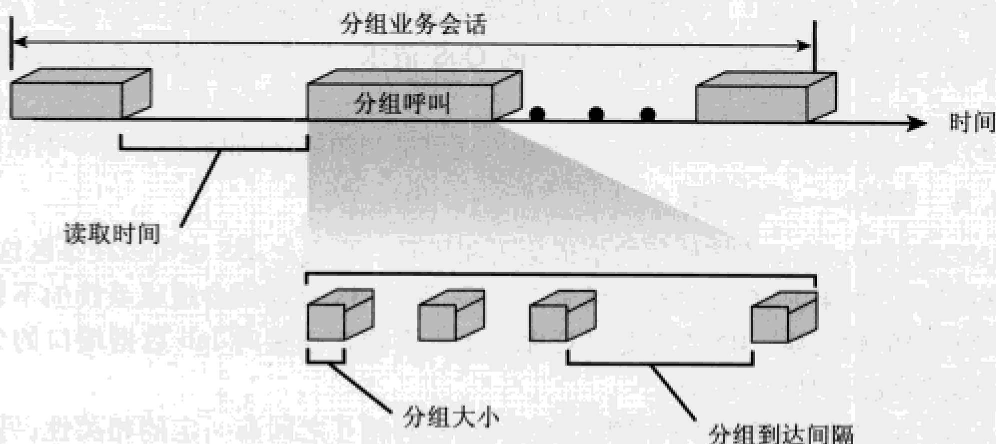


图 5.30 分组业务会话的基本特征

图 5.31 示出了一个基本的分组调度过程。如图所示,分组调度的主要原理和步骤可以总结如下:

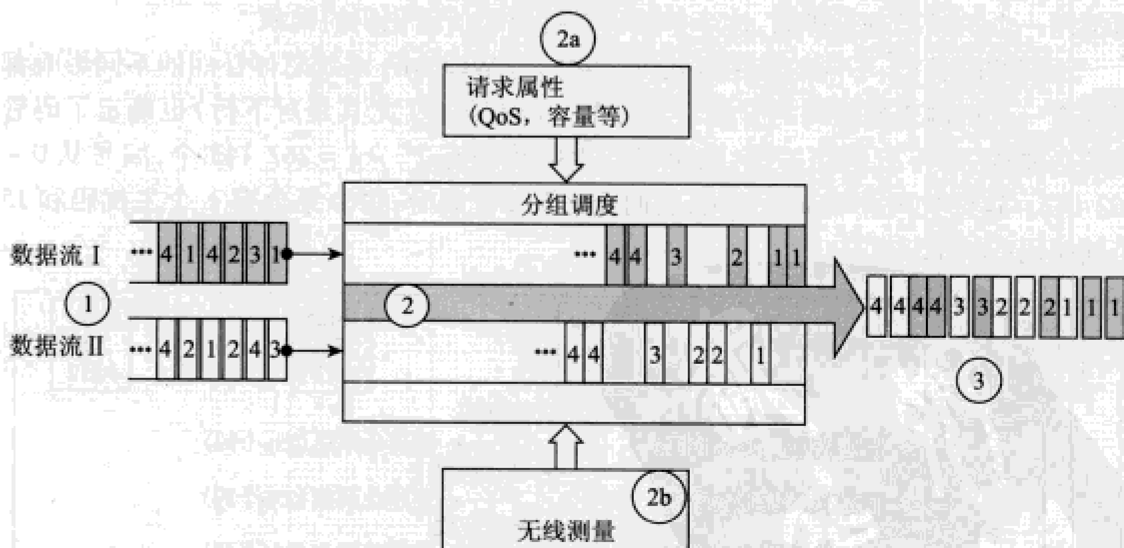


图 5.31 PS(分组调度)的基本原理

(1)RNC 中的 PS(或 HSDPA 的基站)从无线信道接收一个或多个无线链路的数据流。根据所请求的属性以及无线连接的初始链路条件,这些数据流可能已经有完全或部分的优先级排序。但如果有必要的话(如出于无线链路的当前状况等原因),分组调度也可能重排次序。

(2)取出数据分组,并按分组或整个流的原有优先级排序。连接属性由上层协议(2a)提供。映射到当前链路状态及无线物理资源时,所请求的 QoS 格式内容可能满足

也可能不满足。如果能满足，则保留原有次序，并可能将其与无线信道匹配，匹配时考虑到 QoS 要求以及无线信道的特性和能力。如果不能满足预定的 QoS，重新执行 QoS 以及到无线信道的映射。此时重排分组的优先级次序，形成最终的 QoS 数据及对无线信道的匹配，重排需要综合考虑原先的 QoS 请求、当前的链路状态及无线资源状态。

(3)将经过调度和优先级排队后的分组发送到适当的链路(如最利于 QoS 的链路)。

5.3.1.4 RRM——码管理

RNC 管理 Uu 接口连接使用的信道化码和扰码。原则上，BS 也可以在小区这一级管理这些码，但如果 RNC 在进行无线资源管理，那么 BS 管理码会造成系统的不稳定，例如 RNC 级的软切换。RNC 负责码管理也便于多通道连接时 Iub 数据端口的分配。不过，实际生成码的位置是 BS。

Uu 接口的工作需要两种不同类型的码：有些码相互之间有一定的相关性，另外一些是完全不相关的正交码。每一个小区使用一个扰码，UE 通过识别这些扰码来区分系统中的小区。在每个扰码之下，RNC 有一组信道化码，它们对每个扰码都是相同的。BCH 信息是经过了扰码的，因此 UE 接入网络时，首先需要得到正确的扰码。当 UE 和网络之间建立了连接时，信道化码用来区分不同的信道。Uu 接口发送信息时，每个信道都用一个扩频码进行扩频，这个扩频码是扰码和信道化码的乘积。

不同的码类型、不同的使用方式以及它们对 WCDMA 系统总体性能的不同影响都需要有一个机制来控制码的分配与再分配。码有限性(尤其是对下行)也确定了码管理的必要性：对下行链路来说，共可以产生的扰码有 $2^{18}-1=262\ 143$ 个，编号从 0 ~ 262 142。这些扰码并非都会使用，它们分为 512 个集合，每个集合有 1 个主扰码和 15 个辅扰码(见图 5.32)。

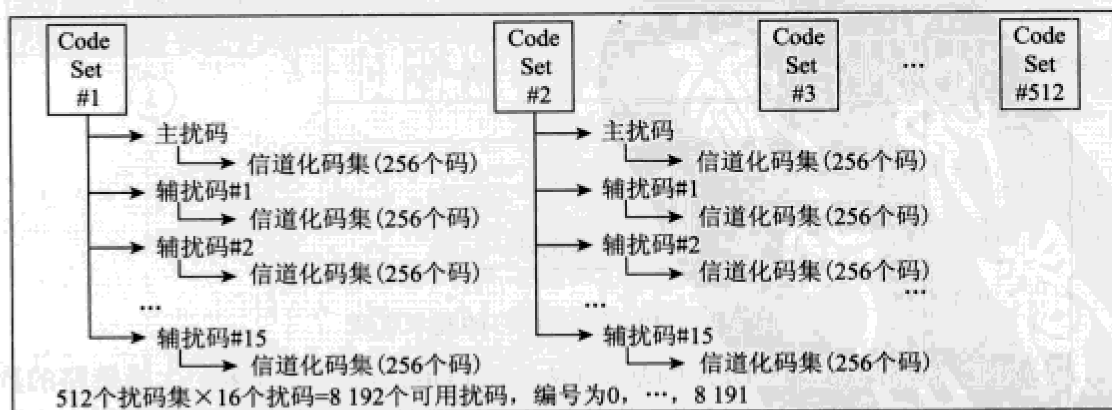


图 5.32 扰码与信道化码的数量及关系

所有编号为 $n=16\times i$ 的扰码组成了主扰码，其中 $i=0,\cdots,511$。第 i 个辅扰码集由编号为 $16\times i+k$ 的扰码构成，其中 $k=1,\cdots,15$。每一个主扰码和每一组辅扰码集之间是一一对应的，第 i 个主扰码与第 i 个扰码集对应。

这样就有 $k=0,1,\cdots,8\ 191$ 个扰码可用。根据 3GPP TS 25.213,每一个扰码可关联到一个偶序号可选扰码和一个奇序号可选扰码,这些扰码可用在压缩帧中。和扰码 k 相关的偶序号可选扰码是 $k+8\ 192$,奇序号可选扰码是 $k+16\ 384$。主扰码集进一步分为 64 个扰码组,每一组由 8 个主扰码构成。第 j 个扰码组由主扰码 $16\times8\times j+16\times k$ 构成,其中 $j=0,\cdots,63$ 与 $k=0,\cdots,7$。

每个小区只分配一个主扰码。主 CCPCH(公共控制物理信道)总使用主扰码进行发射。其他下行物理信道可以采用主扰码或者同扰码集的辅扰码发射。

上行的情况和下行不同,因为上行有上百万的扰码可用。WCDMA 上行链路的扰码数量为 2^{24} 个。除 PRACH 以外,所有的上行信道都可以使用短扰码或长扰码。PRACH 只能使用长扰码。因此在 WCDAM 系统中,上行码分配的问题不像下行那么突出。

无论上行下行,信道化码都用于区分信道。信道化码有不同的 SF 值,因而也就有不同的符号速率。一共有 256 个信道化码可用,SF 值反映连接中使用的码数。SF 值越大,对信道化码和无线资源的利用就越好。高用户数据速率时的 SF 相对较小,因此高速数据会消耗更多空中接口的码容量。

信道化码本质上是正交码。"正交性"意味着这 256 个码组是刻意挑选出来的,以使相互之间的干扰尽可能小。这对于良好的信道区分来说是必需的。另一方面,用于区分用户和小区的码(扰码)必须要有很好的相关特性。信道化码不具有这样的特性,这就是为什么要同时采用扰码和信道化码的根本原因。

每个 WCDMA 小区一般使用一个下行扰码,它在局部是唯一的,起着小区标识码的作用。小区标识码可使用户识别网络,局部唯一性可使 UE 能正确识别无线电波。这种扰码的特点是伪随机的(并不总是正交的)。在此扰码之下,每个小区都有一组信道化码,它们在本质上是正交的,用于信道分离。

5.3.2 UTRAN 控制功能

对于 UTRAN 来说,为了控制和管理 RAB,提供 RAB 业务,除了需要执行 RRM 算法之外,还需要执行一些其他的功能,可以分类为如下几项。

- 系统信息广播。
- 随机接入和信令承载建立。
- RAB 管理。
- UTRAN 安全功能。
- UTRAN 级的 MM(移动性管理)。
- 数据库处理。
- UE 定位。

5.3.2.1 系统信息广播

RNC 的一个重要功能是处理系统信息任务。系统信息用于维护 UE 和 UTRAN 间的无线连接以及控制 UTRAN 的总体运行。RNC 通过广播系统信息来辅助 UTRAN 控制功能的完成,这些系统信息包括无线测量准则、寻呼指示、无线通道信息以及用于定

位的辅助数据信息等。只要 UTRAN 能识别出 UE,不论是处于 IDLE 状态还是处于连接状态,UE 都可以接收到系统信息。系统信息还可以有其他用途,例如用于 CN 提供广播业务。必要时,RNC 可利用点对多点的系统信息广播来维持 UE 和 UTRAN 的联系。

从协议结构来看,系统信息广播功能是 RRC 的一部分,其终结点在 RNC。

图 5.33 示出了系统信息的结构,它和分组类别信息一起使用,形成系统信息分组和排列的基础。如图所示,系统信息单元的组成主要是基于 MIB(Master Information Block,主信息块)、两个可选的 SB(Scheduling Block,调度块)和 SIB(System Information Block,系统信息块),其中系统信息块包含实际的系统信息。3GPP 标准 TS 25.331 定义了 17 种不同的 SIB,其中有的 SIB 也可能包含子 SIB。在一个小区中,MIB 包含有关 SIB 数量的位置排列信息,它也可能包含一两个 SIB 的位置排列信息,后者又包含其他 SIB 的排列信息。因此,只有 MIB 和 SB 包含 SIB 的排列信息。

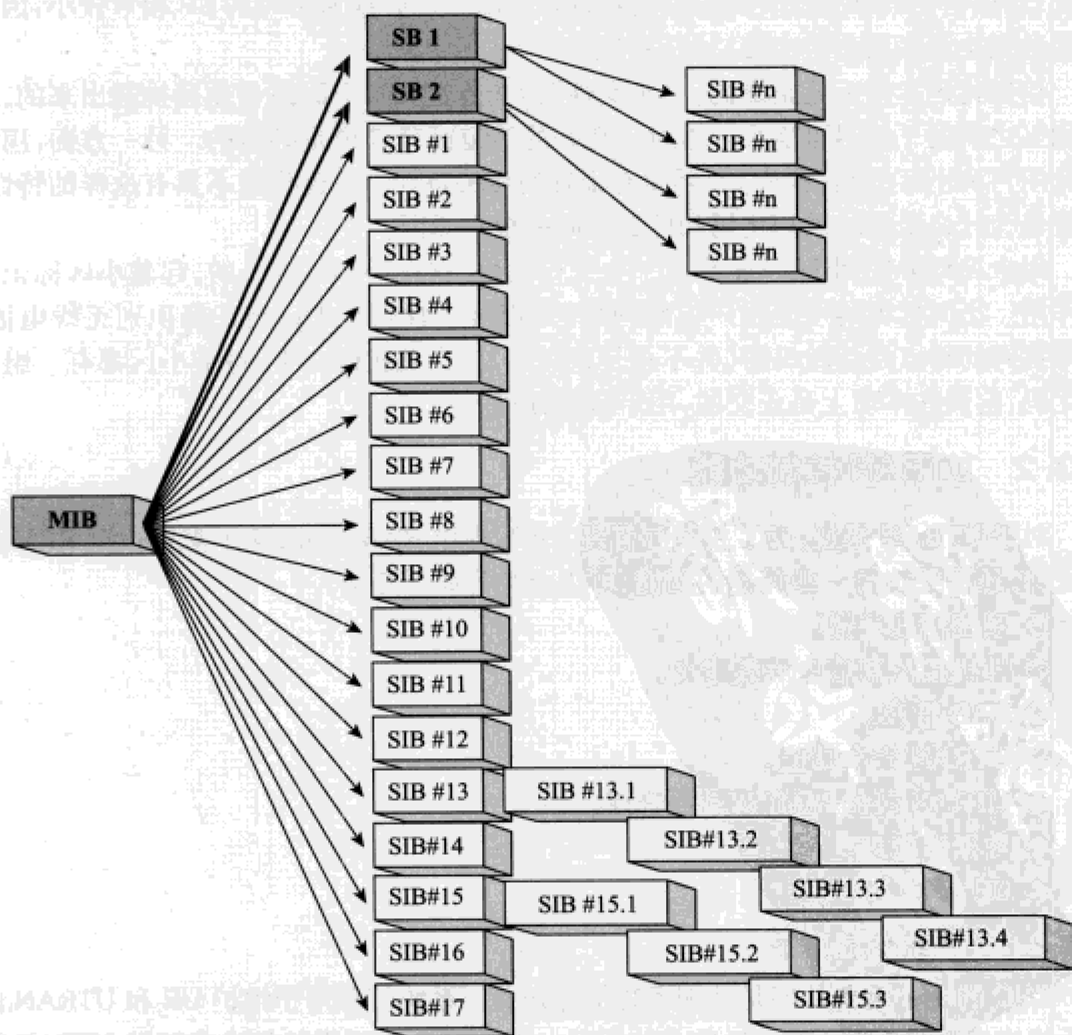


图 5.33 UTRAN 系统信息的基本结构

不同的 SIB 有不同的特性,RNC 将其按重复率和重要程度划分,用于不同的目的。例如 SIB#1 用来向 UE 提供空闲模式和连接模式下的定时器和计数器信息,而 SIB#2 和 SIB#3 用来通知 UE 有关 UTRAN 层的 MM、小区选择和重选等信息。

在需要修改系统信息排列等情形下,RNC 有可能与 BS 一起处理各种结构化过程,不过系统信息的控制功能仍然完全属于 RNC。当 RNC 创建了系统信息数据后,它把信息转发给 BS,然后通过空中接口广播给 UE。根据空中接口的情况,BS 将向 RNC 反馈通过 Uu 接口进行系统信息广播的能力(见图 5.34)。

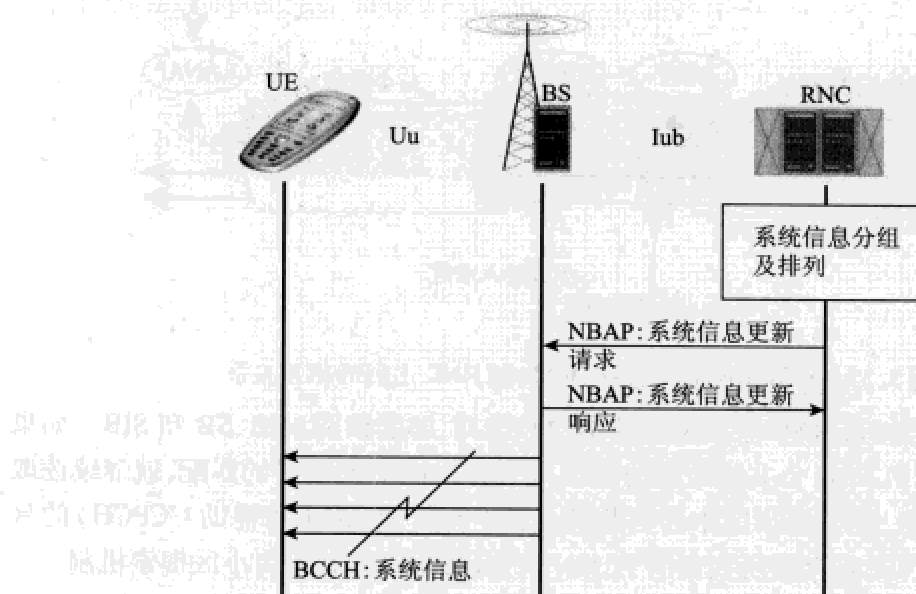


图 5.34 系统信息广播

5.3.2.2 初始接入和信令连接管理

在 RNC 把任何 RAB 映射为 RB 之前,首先需要在 UE 和 CN 之间创建信令连接。3GPP TR 25.990 将信令连接定义为 UE 和 CN 之间的确认模式链路,用以传输 NAS(非接入层)的高层信息。为了实现这个功能,RNC 利用 RRC 连接业务在 UE 和 UTRAN 之间创建 SRB(Signaling Radio Bearer,信令无线承载),以提高信令连接中的传输业务。一旦 RNC 创建了 SRB,RNC 将使用第一个 RLC RB 来转换和传输从 UTRAN 到 UE 的信令连接(注意 RB 是 RLC 层提供的业务,用于在 UE 和 RNC 之间传输用户数据)。不过也可以用主 RB 来进行信令连接,如图 5.35 所示。

UE 打开电源进入空闲模式后将会试图与 UTRAN 取得联系。UE 在 UTRAN 中寻找合适的小区,选择出能提供相应业务的小区,然后调谐到该小区的控制信道。此时称为"驻留在该小区"。驻留过程包括小区搜索,其中,UE 寻找小区并确定出该小区的下行扰码和帧同步。小区搜索是通过多个步骤完成的。

在小区搜索的第一步是 UE 使用 SCH(Synchronisation Channel,同步信道)的主同步码来获得小区的时隙同步,其中主同步码对所有小区来说都是相同的。第二步,UE

使用同步信道的辅助同步码来获得帧同步,并且识别出第一步找出的小区的码组。在最后的第三步中,UE确定出该小区所使用的主扰码。识别出主扰码后,UE就能检测到PCCPCH,从而获得RNC在该小区的广播信息。

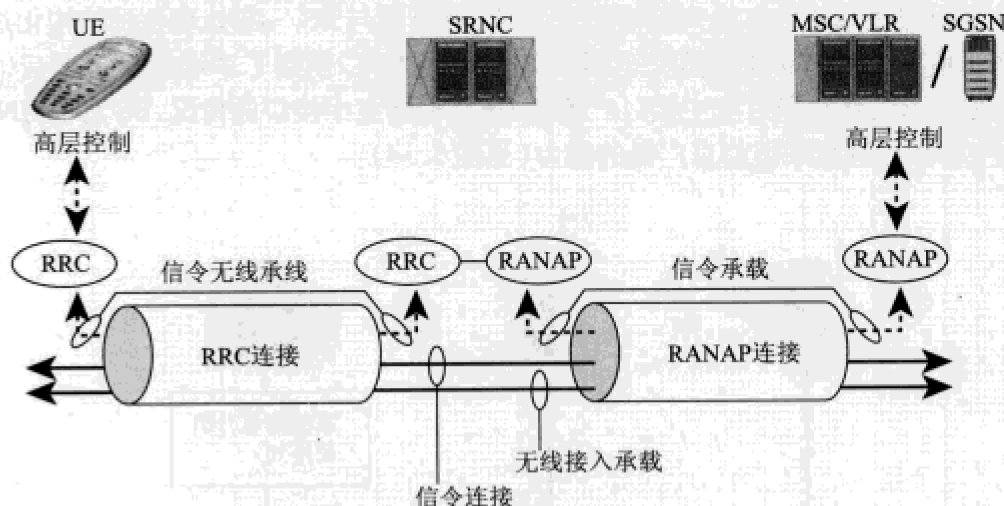


图 5.35 SRB、RB、信令连接、RAB 和 RNC 之间的相互关系

为此,UE应当知道RNC系统信息的结构和排列,即能识别MIB、SB和SIB。如果BCH上MIB中的PLMN(公共陆地移动网络)识别码与UE所搜寻的匹配,就继续读取BCH中的其他信息,例如该小区中公共物理信道(包括PRACH和辅助CCPCH)的具体配置参数,否则UE将存储所找到的PLMN识别码以备用,并重启小区搜索机制。

对UE来说,搜索第一个小区通常是最困难的,因为需要扫描很多扰码才能找到正确的那个。当UE具备捕获某个RNC所控制的BS所必要的信息后,就可以发出初始接入UTRAN的请求信息,从而使UE的状态从空闲模式转变为连接模式。

在这一点上,RNC所涉及的控制功能包括系统信息广播以及控制那些和初始连接相关的BS。此后RNC将主动控制接入过程,负责处理用户通过RACH提出的RRC连接建立请求消息。通过检查UE标识、RRC连接请求的原因和UE的处理能力(它用于RNC为该UE分配初始的信令RB),RNC在这里起着核心作用。RNC根据这个信息决定是否分配信令RB给UE,这个信令RB用来传输初始接入所需要的其余信令并提供后续的相关业务。如果RNC未接受接入请求,UE将在预定的时间段内重启初始接入过程。

无论高层业务请求来自哪个方向,创建SRB的RRC连接请求都是由UE发起的,具体如图5.36所示。RNC收到RRC连接建立请求后将在Iub接口上建立起一个无线链路,连至UE的目标基站。这里无线链路是指单个UE和单个UTRAN接入点之间的一种逻辑关系,它的物理实现包括一个或多个RB传输。如果这一步成功,RNC将通知UERRC连接已建立,UE将作出表示RRC连接完成的响应。

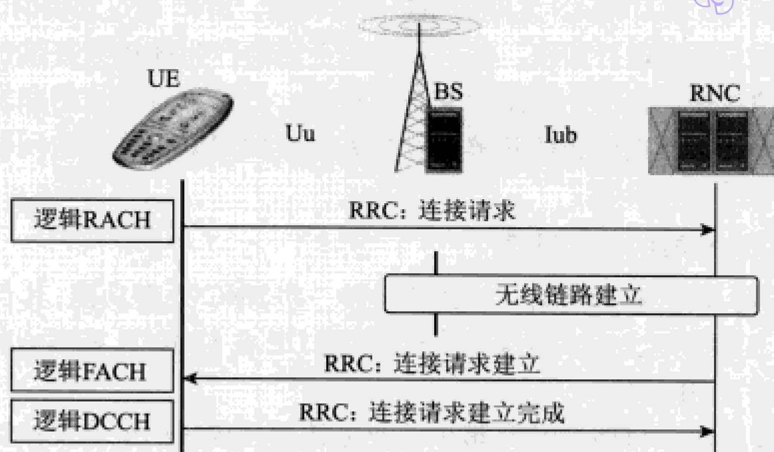


图 5.36 RRC(无线资源控制)连接建立

此时 RNC 和 UE 之间的 SRB 已经准备就绪，因此 RNC 可以转换且传送 UE 与 CN 之间的信令连接及 RAB。需要指出的是，不管 UE 和 CN 之间有多少信令连接和 RAB，RNC 只使用其中一个 RRC 连接来在 UE 和 UTRAN 之间控制和传输它们。基于信令连接和需要传送的 RAB 的数量，RNC 可以重新配置所需的低层服务。

5.3.2.3 无线承载管理

在无线网络和 UE 之间建立好前述的 SRB 后，RNC 将 UTRAN 和 UE 之间把请求的 RAB 映射成 RB 进行传输。这样一来，就好像在 CN 和 UE 之间有一个固定的承载。

UE 和 CN 通过信令连接协议好请求的 RAB 后，将转发至 RNC 做进一步处理。在这里，RNC 的主要功能是分析请求 RAB 的属性、评估所需的无线资源、通过低层服务激活或者重新配置无线信道以及把请求的 RAB 映射为无线承载。因此，RNC 覆盖了所有用于支持 RAB 以及相关无线资源配置的控制功能。

如图 5.35 所示，RAB 在无线接口上的传输是在 RNC 和 UE 之间的 RRC 连接上进行的，在 Iu 接口上的传输在 RNC 和 CN 之间的 RANAP(Radio Access Network Application Part，无线接入网应用部分)协议连接上进行的。RNC 的作用是在 RAN 和 CN 之间的一种协议转换器。RNC 通过现有无线资源信息把请求的 RAB 映射为 RB，并且控制底层的业务。

为了优化无线资源的使用，并共享不同运营商的带宽和网络物理资源，UTRAN 可以支持 NAS 消息的 CN 分配功能。为此，RRC 协议在接入网内以直接传输的方式透明传送 CN 消息。此时，这些消息带有特定的 CN 指示码，UE 和 SRNC 中的分配功能实体根据该指示码把消息定向到恰当的 CN，反之亦然。这样，UE 域和 CN 域都能达到相应的 MM。

5.3.2.4 UTRAN 安全

无线连接安全是 RNC 需要处理的另外一个重要功能。RNC 涉及完整性校验和加密两种功能。完整性校验用来保护 UE 和 UTRAN 之间无线接口上的信令连接，而加

密机制用来保护 UE 和 UTRAN 之间的用户数据传输。RNC 通过预设的完整性和加密算法对信令和用户数据进行加密。在这种情形下需要产生随机数并维护一个和时间相关的计数器值以便进行信令信息的完备性检查。另外也需要使用和发送信息相同的算法对接收到的信息进行验证和解密。有关完整性和解密算法的问题将在第 9 章的 UMTS 安全性中详细介绍。

5.3.2.5 UTRAN 层的移动管理

UTRAN 层的 MM(移动管理)主要指这样一些 RNC 处理功能,其目的在于保持 UE 和 UTRAN 无线小区之间的联系,并能考虑到 UE 在 UTRAN 范围内的移动性以及所使用的业务或 RAB 类型。

如 5.3.1 节所述,UMTS 网络环境中的业务特性和传统的电路交换型业务很不相同。这意味着 UTRAN 能使不同 QoS 的 RAB 共享无线资源。因此需要更先进的机制以便高效地使用有限的无线资源,并且尽可能满足不同 RAB 的 QoS 要求。为了这一目的,RRM 算法需要同 2G 更具适应性的 MM 配合。

因此,UMTS 专门定义了 RRC 状态转移以及分级 MM 的概念,包括 UTRAN 级的 MM,它有 CN 子系统负责,和 GSM MM 相比是一个全新的系统。这样,UE 在无线连接中将有不同的状态,取决于到 UTRAN 的连接类型和 UE 的移动速度。RNC 根据 UE 的移动性、UE 要求的 RAB 以及比特速率变化来控制 UE 的状态。

UTRAN 级移动性的基础是小区的概念、URA(UTRAN Registration Area,UTRAN 注册区)以及 U-RNTI(Radio Network Temporary Identifier,UTRAN 无线网络临时识别码)。另外,为 RNC 定义出不同的逻辑角色并制定 Iur 接口的主要目的也是为了支持 UTRAN 内部的 MM。

一个 URA 是指一个包含许多小区的区域,它只存在于 UTRAN 内部,对 CN 是不可见的。这就是说,当 UE 有一个 RRC 连接时,UTRAN 能在 URA 级别上知道 UE 的具体位置。UE 每次进入新的 URA 时,都必须执行 URA 更新过程。有 RNC 间的接口来支持 URA 过程,原则上可以覆盖不同的 RNC 区域。

根据 3GPPTS 25.401,RNTI(无线网络临时识别码)用于 UTRAN 内 UE 和 UTRAN 间的信令识别 UE。主要有 4 种类型的 RNTI 用于处理 UTRAN 内部的移动性,具体为以下几项。

- S-RNTI(SRNC RNTI)。
- D-RNTI(Drift RNC RNTI)。
- C-RNTI(Cell RNTI)。
- U-RNTI(UTRAN RNTI)。

S-RNTI 是在 RRC 连接建立的同时分配的,由与 UE 建立 RRC 连接的 SRNC 执行。SRNC 通过 S-RNTI 识别 UE,从而能使其访问 UE。

D-RNTI 由 DRNC 在报文建立时分配,用于处理 UE 的连接和 Iur 接口上的报文。

C-RNTI 是在 UE 接入一个新的小区时分配的,它是一种 CRNC 特定的识别码,用

于识别该 UE 的 RRC 所连接的 CRNC。就是说,CRNC 通过 C-RNTI 识别 UE 并可访问 UE。这个识别码用于 UE 处于小区的前向接入信道(FACH)状态时。

U-RNTI 则是分配给具有 RRC 连接的 UE 作为 UTRAN 内的 UE 识别码,用于 UE 已经存在 RRC 连接时的初始接入(小区改变)以及 UTRAN 主叫(包括相关的响应)的情形。

分配和处理上述识别码是 RNC 的主要功能。

有了 RNC 的作用、UE 识别码和 URA 的概念,我们来看这样一个问题,就是为了处理 UTRAN 内部的移动性和 RRM 功能,如何将上述概念同状态转移结合到一起。图 5.37 示出了处理 RRC 状态转移的主要原理,总结如下。

- 没有无线连接:UE 的位置只有 CN 知道(准确到位置区或路由区,这是 CN 级的位置区概念,将在第 6 章详细介绍),因此位置信息存储在网络中,它是 UE 最近一次对 CN 的 MM 事件的结果。
- 公共信道上的无线连接:如果无线连接使用公共信道,例如 FACH 和 CPCH 信道,那么 UE 的位置可以准确到小区级别。UE 的位置信息通过 RRC 中的小区更新过程进行更新。此过程可用于 UTRAN 和 UE 之间的低比特速率数据传输。
- 专用信道(DCH)上的无线连接:此时 UTRAN 对该连接分配了专用资源,至少是 1 个 DPDCH 和 1 个 DPCCH,根据所需带宽,可能有多个 DPDCH。UE 的位置准确到小区级别。根据链路连接的类型不同,可能会执行不同的 RRC 过程。如果专用连接用于传输具有高 QoS 等级的业务(例如电路交换语音业务),UTRAN 和 UE 将执行切换;如果业务是允许缓存和延迟的低 QoS 等级的,例如网页浏览,不一定执行切换操作。UE 将通过小区更新过程来通知 UTRAN 它的位置信息,即告诉 UTRAN 无线连接上的数据应该发送到什么位置。
- 无线连接处在小区寻呼信道(PCH)状态:若 UE 处于小区 FACH 或者处于小区 DCH 状态但无数据传输时,UE 的状态将改变为小区 PCH 状态,这样 UE 可按预定的 DRX(Discontinuous Reception,不连续接收)周期监听可能发生的寻呼。此时,UE 的位置能够准确到单个小区,有时候也把该小区称为归属小区。
- 无线连接处在 URA PCH 状态:若 UE 处于小区 FACH 或者小区 DCH 状态,但没有多少数据需要传输或者 UE 处于高速移动状态,那么 UE 的状态可以转移为 URA PCH 状态。这是为了避免周期性的小区更新操作,释放相应的无线资源。此时 UE 的位置信息准确到一个 URA 范围内,如欲获得小区级的定位信息,应由 UTRAN/RNC 对 UE 进行寻呼。移动台定位过程采用了基于小区的定位时就会出现这种情况。在 URA PCH 状态下,RNC、URA 之间的 Iur 接口对 UTRAN 起到很好的作用。
- 闲置模式:RRC 的闲置模式等同于 UE 和 UTRA 之间没有任何链路连接的状态(如同 UE 关机)。在这种 RRC 模式下,网络没有任何关于 UE 位置的有效信息。

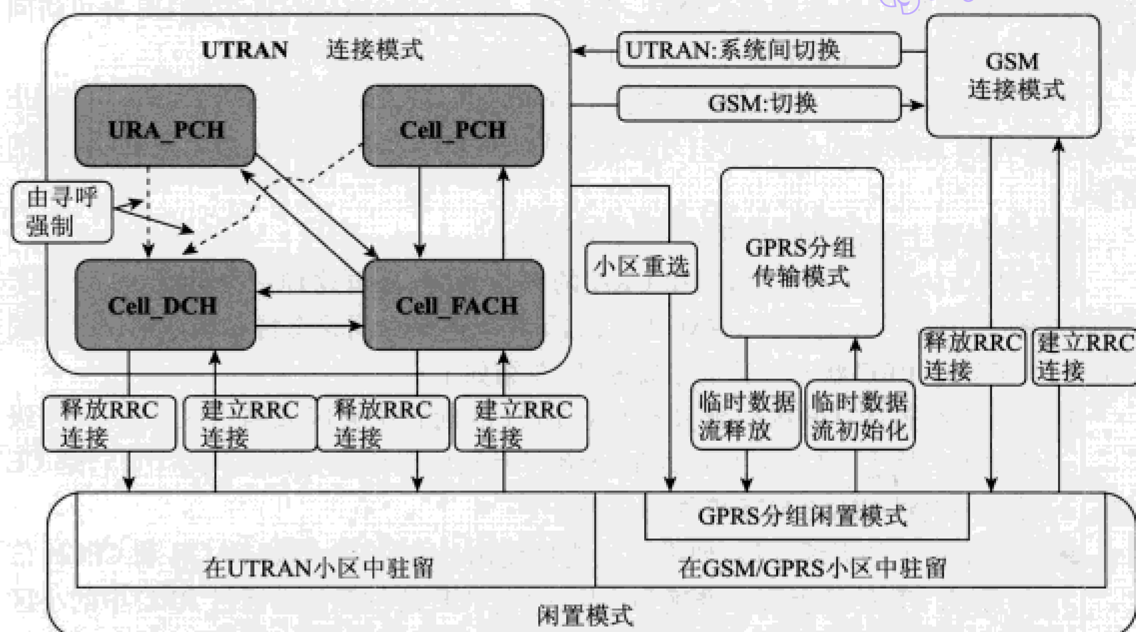


图 5.37　包括 GSM/GPRS 连接选项的 RRC 状态转移图

5.3.2.6　数据库处理

类似于 GSM 的 BSC，RNC 存储了各种信息，称为无线网络数据库。RNC 所控制的小区信息存储在这个数据库中。RNC 把相关的信息发送给对应的小区，这些小区又把这些信息通过 Uu 接口广播给 UE。无线网络数据库包含了大量和小区相关的信息，小区所用的码只是其中的一部分。

无线网络数据库中存储的信息大致可以分为以下几部分。

- 小区识别信息：码字、小区识别码、位置区识别码和路由区识别码。
- 功率控制信息：在小区覆盖范围内的上行和下行方向允许的发送功率等级。
- 与切换相关的信息：UE 触发切换操作所需要的连接质量以及业务相关的参数。
- 环境信息：邻小区信息（包括 GSM 和 WCDMA）。RNC 将这些小区列表发送给 UE，UE 可执行无线环境测量以便为切换做准备。

5.3.2.7　UE 定位

RNC 执行的另外一个重要功能是控制 UTRAN 中 UE 的定位机制。RNC 选择合适的定位方法，并控制这些方法在 UTRAN 和 UE 端的执行方式。RNC 也负责协调执行 UE 定位功能所涉及的 UTRAN 资源。

在基于网络的定位方法中，RNC 估算 UE 的位置并指示估值的准确性。为了定位或协助定位 UE，RNC 需要控制许多位置测量单元（Location Measurement Unit）或基站以进行无线测量。

由于在 UNTS 网络中 UE 定位可以看成是一种增值业务，所以我们在后面的第 8 章中将详细讨论定位业务的具体实现。

第 6 章 UMTS 核心网

UMTS CN(核心网)可看作是向 UMTS 用户提供所有通信业务的基础平台。基本的通信业务包括电路交换呼叫业务和分组数据路由业务。3GPP R5 也引入了一个新的系统,称作 IP 多媒体子系统(IMS)。通过无缝地集成移动领域和因特网领域,并提供能用于移动通信的成熟业务机制,IMS 为移动应用开创了基于 IP 协议的业务领域。

CN 把端到端的 QoS 要求映射到 UMTS 承载业务中。当与其他网络互连时,QoS 要求也需要映射到可获得的外部承载业务中。在创建端到端的业务通路时,UMTS CN 的网关功能如图 6.1 所示。外部网络的承载业务不在 UMTS 系统标准范围内,所以如果 UMTS 和外部网络的 QoS 请求不匹配时,就会在本地网络引起一些问题。



图 6.1　CN 中的承载和 QoS 体系

在 MT(移动终端)和 CN 之间,QoS 由无线接入承载业务提供。无线接入承载对 CN 掩盖了无线路径上的 QoS 操作。在 CN 中,QoS 要求被映射在自己的承载业务上,它又装载于物理承载业务之上的骨干承载业务上。CN 实现的一大挑战是营运商可以自由选择怎样来实现物理骨干网承载。物理骨干网承载依赖于 CN 节点之间使用的物

理传输技术。可以选择典型的传输技术,比如 PCM 信道或 ATM 信元交换的 PDH 和 SDH 技术。3GPP R5 中的重点就是在可能的时候用 IP 替换这些技术,因为统一的传输网能简化高端协议层的功能。

UMTS 体现了这样一种思想,就是用统一的核心来处理大量不同的无线接入。回顾第2章所讨论的网络演化过程,3GPP R5 目前认可三种无线接入技术:WCDMA/HSDPA、GSM/EDGE 以及可能的补充接入技术。在这几种技术中,WCDMA/HSPDA 与 GSM/EDGE 已经实现,而补充接入技术还在研究当中。UMTS 网络核心部分的演进不像无线网络那样直接,这是因为 CN 的传统结构基础以及先进的技术对 UMTS 核心部分的演化有着许多不同的影响。图 6.2 表示了 UMTS CN 的基本概念:实线是开头使用的无线接入技术,其他是以后候选的接入技术。

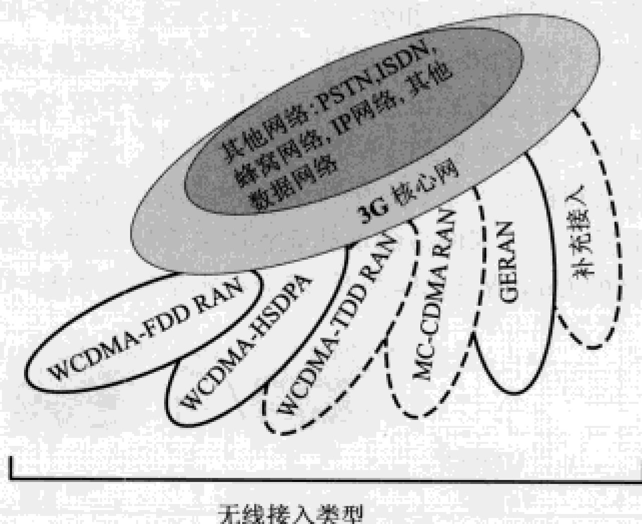


图 6.2 对无线接入统一的核心网

6.1 UMTS 核心网结构

3GPP R99 为接入网引入了新的机制且提高了容量。从 3GPP R4 开始到 3GPP R5 中的实际实现,CN 经历了许多重要的变化。本章简要讨论 3GPP R5 的主要特点。

如图 6.3 所示,UMTS 核心网由一些称作“域”和“子系统”的设备实体构成,它们的目的是描述设备所关注的业务特点。按照这种分法,UMTS CN 包括下面几种实体。

- CS(电路交换)域。
- PS(分组交换)域。
- IMS(IP 多媒体子系统)。
- BC(广播)域。

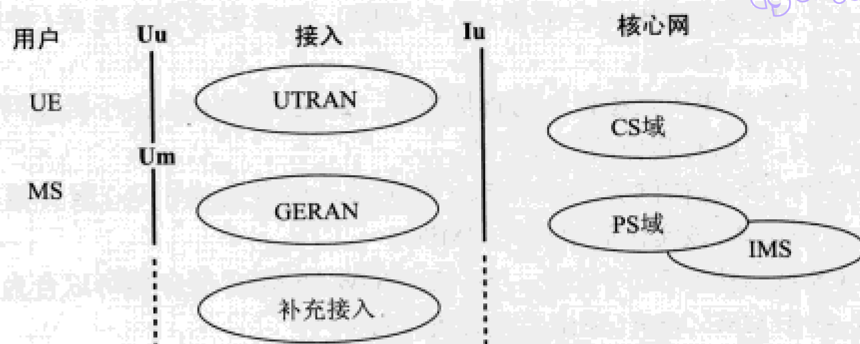


图 6.3 域/子系统级的 CN 结构

从 CN 的角度来看，域和子系统之间有什么区别呢？CN 域是直接与一个或多个接入网连接的接口。这种接口称作“Iu”。鉴于业务属性并为了标识域，Iu 通常都是带下标的。例如，Iu_{CS}是接入网与 CS 域的接口，它传输 CS 业务；Iu_{PS}则是用于 PS 业务的接口；而 Iu_{BC}是承载广播或多播业务的接口。CN 子系统和接入网之间没有直接的 Iu 类型接口，它们利用另外定义的接口与一个或多个 CN 域相连。

图 6.4 的目的是解释在 UMTS CN 中最重要的接口。如果想了解其全部内容，可以参考 3GPPTS23.002，版本 5.12.0。

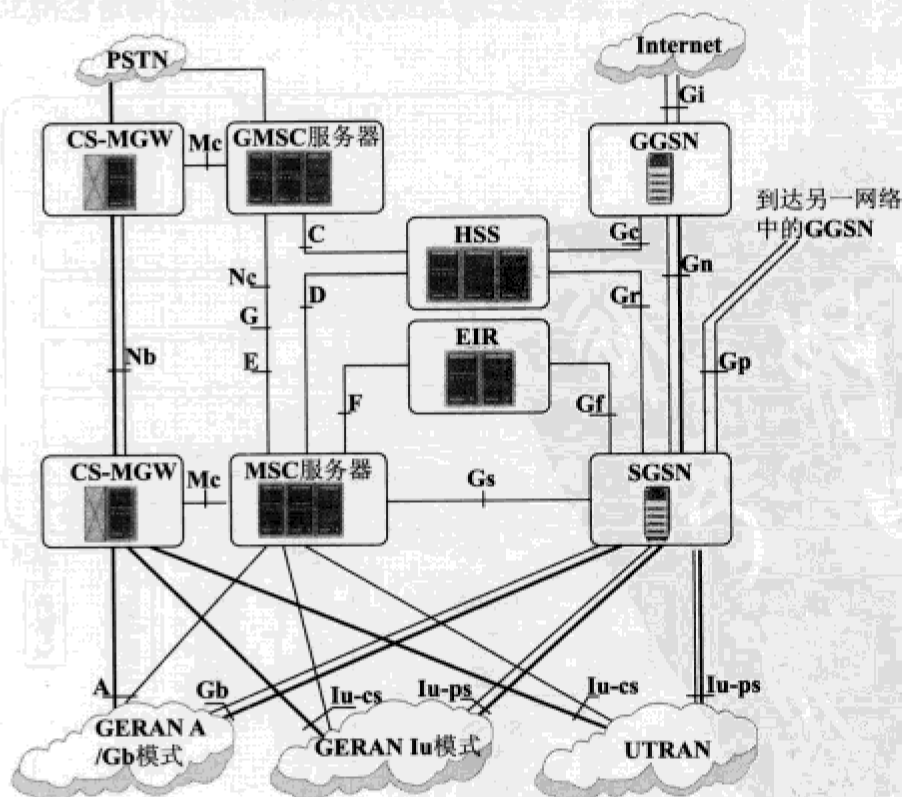


图 6.4 支持电路交换和分组交换业务的核心网构架

在图 6.4 中，粗线条表示用户业务（用户平面），细线表示信令连接（控制平面）。关于 CN，需要指出下列几点。

- 图中所画的连线代表逻辑上的直接连接。但在实际当中，由于传输网的解决方案的原因，可以有其他的连接方式。
- CS-MGW（CS 媒体网关）和 GMSC（网关移动业务交换中心）服务器可以合为一个物理实体，该实体简单称作 GMSC。
- 如果 CS 域结构和 3GPP R99 一致，CS-MGW 和 MSC 服务器可以合为一个物理实体，称作 MSC/VLR（来访者位置寄存器）。
- 如果服务 GPRS 支持节点（SGSN）和 MSC/VLR 合并成一个物理实体，则称作 UMSC（UMTS MSC）。

6.1.1 节～6.1.3 节将介绍和 CN 域相关的问题。IMS 的内容在 6.4 节～6.6 节介绍。

与 CN 管理任务和控制任务相关的问题，比如身份标识和寻址，将在 6.2 节介绍。

6.1.1 域和子系统的通用核心网实体

除了这些域外，CN 还包含一些对所有 CN 域和子系统都通用的功能。这些通用功能主要集中在一个叫作 HSS（归属用户服务器）的实体中。

图 6.5 并没有包括 BC 域。尽管它已被定义为 CN 的一部分，但是它在 3G 网络中的实现还需要进一步的研究。

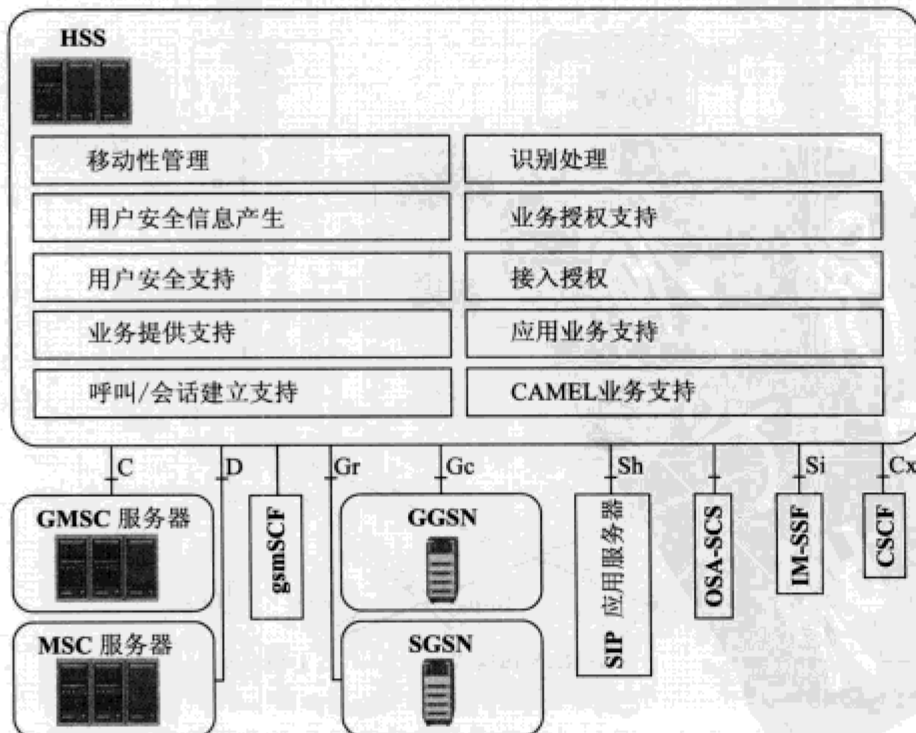


图 6.5 归属用户服务器的功能及其对核心网域的接口

从图 6.5 中可以看到,大部分 HSS 功能已经在网络中存在了很长时间。以前它们由独立的单元负责:如 HLR(归属位置寄存器)和 AuC(鉴权中心)。在 3GPP R5 结构中,HLR 和 AuC 被视作 HSS 的子集,但是它们仍然提供相同的功能。

- MM(移动性管理)功能通过 CS 域、PS 域和 IMS 域支持用户的移动性。HSS 在这方面的作用是存储寻址信息以在 MM 级内定位出用户/终端的位置。
- 用户安全信息的产生、用户安全支持和接入鉴权,这些功能主要由 AuC 子集负责,该子集通过 HLR 子集发送信号到 CN 域和子系统。
- 业务提供支持:HSS 提供到业务配置数据的访问,这些数据用于支持 CS 域、PS 域和/或 IMS 应用服务以及 CAMEL(移动网络定制应用增强逻辑)业务。HSS 通过与 SIP(会话初始协议)AS(应用服务器)和 OSA/SCS(开放业务体系/业务能力服务器)进行通信来支持 IM CN 子系统中的应用业务。HSS 还通过与 IM-SFF 通信来支持与 IM CN 子系统相关的 CAMEL 业务,通过与 GSM SCF 通信来支持 CS 域和 PS 域中的 CAMEL 业务。
- 呼叫/会话建立支持:在 CS 域、PS 域和 IMS 中,HSS 支持呼叫和/或会话建立过程。当业务终止时,它可以提供承担呼叫/会话控制实体的相关信息。
- 标识处理:HSS 为所有唯一标识用户的标识码提供合适的关联:包括 CS 域的 IMS 和 MSISDN,PS 域的 IMSI、MSISDN 和 IP 地址,IM CN 子系统的私有标识和公共标识。6.2.1.1 节将进一步详细介绍。
- 业务鉴权支持:HSS 对 MT 的呼叫/会话建立和业务请求提供基本鉴权。并且还可以根据提供给用户的相关业务信息更新至合适的服务实体。

除了 HSS,EIR(设备标识寄存器)也是一个所有域和子系统公用的功能。EIR 存储关于终端用户设备的信息和设备的状态。它利用三个“名单”来实现这一功能,简单地说:白名单包含许可的正常终端设备的信息,黑名单存储失窃设备的信息,而灰名单包含关于嫌疑设备的序列号信息。黑名单和灰名单通常会使用,而白名单不经常使用。EIR 维护这些名单并在有要求时向 CN 域提供有关用户设备的信息。如果 EIR 指示该终端设备在黑名单中,CN 域就拒绝传输业务到该终端或接收来自该终端的业务。如果终端设备在灰名单中,系统会传输其业务正常,但会进行跟踪报告。

6.1.2 电路交换域

3GPP R5 包含了 CS 域,因为后向兼容要求网络必须支持 CS 业务。3GPP R99 引入了 CS 域结构,该结构从 GSM(移动通信全球系统)中直接继承下来。3GPP R4 的 CS 域结构有一个替代实现方案,可使运营商能分别调整 CS 域控制和业务传送容量(见图 6.6)。

CS-MGW-MSC 服务器划分的主要目的是在 CS 域中分离控制平面和用户平面。这就给系统带来了可扩展性,因为单个 MSC(分布式移动交换中心)服务器可以控制许多 CS-MGW。分布式 CS 域结构的另一个优点是它可以优化用户平面的地理结构。

例如,运营商可以在网络内自由地设置 CS-MGW 的位置,通过恰当的路由安排,可以让用户平面以最短的地理途径通过网络。CS-MGW 也可以包括不同的转换包,可以使运营商对传输网进行优化配置。例如使用 CS-MGW 思想后,运营商可以在 CS-MGW 的接入网侧和现有 PSTN(公众电话交换网)侧把 CS 域骨干网从其他传输技术转换成 IP 网。

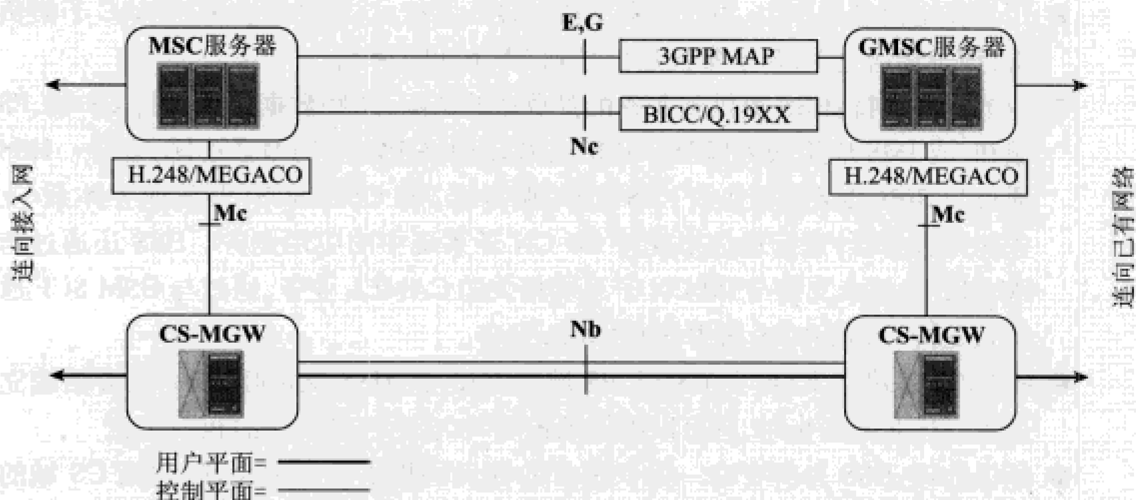


图 6.6　带有分布式移动交换中心功能的 UMTS 核心网电路交换

3GPP R4 分布式的 CS 域体系也定义了 MSC 的划分,呼叫控制功能和 VLR 在"MSC 服务器"实体中,用户平面连接性及其他事项(如网络互连)在"媒体网关(MGW)"实体中。整个 CN 中有各种各样的网关,因此最好在 MGW 之前加上前缀"CS"以清楚地表明我们谈论的是 CS-MGW(电路交换域的媒体网关)。

MSC 服务器和 CS-MGW 分离后,CS 域内便有了一个新的接口。该接口(Mc)使用ITU-TH. 248定义的媒体网关控制协议(MGCP)。H. 248 只形成了该接口中信息传输机制的基础,完全实现还要包括各种与 3GPP 相关的扩展。Mc 接口包括呼叫不相关和呼叫相关的 H. 248 事件。该接口中呼叫不相关的事件包含将 CS-MGW 的功能状态传送到 MSC 服务器的控制机制。呼叫相关的事件可视为一个信封,它传输来自接入网用户或者来自固网的控制平面信息。呼叫相关及呼叫不相关事件最早定义在 3GPP TS29. 232 版本 5. 0. 0 中。

Nc 接口携带网络到网络的呼叫控制信息。原则上说,只要支持呼叫承载与其控制流独立,任何控制协议都可以。3GPP 采用的是 BICC(与承载无关的呼叫控制协议)。准确地讲,BICC 并不是一个单一的协议,而是一些包的集合。这些包主要是在 ITU-T 标准 Q. 1950"与承载无关的呼叫承载控制协议"中定义的。

Nb 接口携带用户平面和传输网控制平面。在用户平面端,Nb 接口包括用于数据传输的适当帧协议和其他机制。根据相关标准,Nb 接口可以使用 ATM 传输或 IP 传输来实现。这两种传输方式最早见于 3GPP TS29. 414 版本 5. 0. 0。

MSC 服务器之间当然也需要相互进行通信。出现这种情况的因素有很多,如在 GERAN(GSM/EDGE 无线接入网)中的 MSC 到 MSC 的切换,在 UTRAN(UMTS 的地面接入网)中的服务 RNC(无线网络控制器)重定位等。在这些情况下,用户业务的控制从一个 MSC 服务器转移到另一个 MSC 服务器,在接入网边缘的 CS-MGW 也随之改变。这就是为什么 MSC 服务器需要有 MAP(移动应用协议)接口 E 和接口 G,这两个接口在 MSC 服务器之间传输 MM 和其他相关的信息。关于 MAP 的详细资料请参见 3GPP TS29.002。

多少有些奇怪的是,3GPP R5CS 域并不一定要按照 EGPP R4 的指导来实现,它允许在网络的 CS 端继续按 3GPP R99 实现。此时的 CS 域直接继承了 GSM,沿用 GSM 的传统功能。这种方法的优势在于对网络投资的需求会减少。不过也有其缺点,在 CS 域中保持 3GPP R99 结构将影响运营商对网络的可扩展性。另外,这种方案也不能达到最佳的用户平面路径,因为控制平面和用户平面没有严格分开。

6.1.3 PS 域

PS 域中最主要的两个元素是两种移动网络特有的服务器:SGSN(GPRS 服务节点)和 GGSN(GPRS 网关节点)。

SGSN 包含了位置寄存器的功能,它维护主叫或被叫分组数据传输所需要的数据。这些数据是一些用户信息,包括 IMSI(国际移动用户识别码,见 6.2.1.1 节)、各种临时识别码、位置信息(见 6.2.1.2 节)、PDP(分组数据协议)地址(实际中就是 IP 地址,但可以不是)和用户预订的 QoS(参阅第 8 章)等等。

PS 域中用于数据传输的工具是“PDP 报文”(见 6.2.2.2 节)。为了传输数据,SGSN 必须要知道在哪个 GGSN 上存在某终端用户激活的 PDP 报文。因此 SGSN 必须存储每个激活 PDP 报文的 GGSN 地址。注意 SGSN 上的多个激活 PDP 报文可能会经过多个 GGSN。

GGSN 也有一些用户数据,可能包括 IMSI 号、PDP 地址、位置信息和用户所注册的 SGSN 信息。

对于 PS 域的体系来说,光有 SGSN 和 GGSN 是不够的。分组业务中的寻址、安全和计费都需要其他一些元素和功能。图 6.7 显示出 PS 域中最相关的一些功能。

出于安全考虑,运营商目前为终端用户采用动态地址分配。分配地址的方法很多,一般都是采用 DHCP(动态主机配置协议)功能服务器。基于运营商的配置,DHCP 为终端用户的终端设备分配 IPv4 或 IPv6 地址。

在某种程度上 PS 域实际是一个成熟的内联网。为了在内联网内对不同的单元进行寻址,就需要 DNS(域名服务器)。PS 域中的 DNS 主要任务是对 PS 域中的单元进行寻址。例如,当 SGSN 对某一特定的 GGSN 建立业务时,SGSN 从 DNS 请求所需的 GGSN 地址。

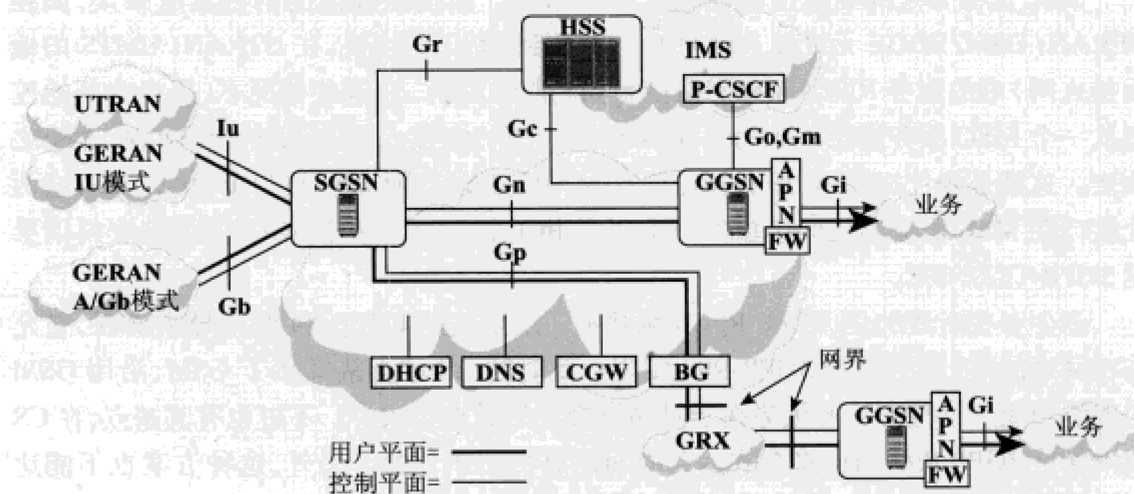


图 6.7 分组交换域结构示意图

当用户获得了动态分配的地址,并且在 SGSN 和 GGSN 之间已经建立了连接后,用户就可以接入运营商开通的业务。业务接入是通过 APN(接入点名称)来安排的,APN 可以自由定义但一般与业务相关。例如,APN 可以是"Internet",通过这个 APN 用户就可以在因特网上浏览。再比如,名为"WAP"的 APN 能够使终端用户浏览运营商提供的 WAP 菜单。GGSN 可能包含成千上万个 APN 定义:它们可能是一些公司/企业,可能在任何地方、任何网络上。如果运营商不愿意使用这种接入控制方式,也可以采用"万能卡(wild card)"APN 方式。此时允许终端用户连到任何自己想连的地方,运营商只是提供连接。

考虑安全问题,GGSN 集成了 FW(防火墙)。为了保证终端用户业务的安全,每个到 PS 域的连接都要经过 FW。

大多数网络都有 PS 域,因此这些网络之间的漫游问题起码从商业来说是非常重要的问题。PS 域有一个单独的功能可以实现漫游,使两个不同网络的 PS 域实现互连。该功能也称为"BG(Border Gateway 边界网关)"。GRX(GPRS 漫游交换)是为了通用分组无线业务漫游目的而提出和实现的。

为了进行计费数据的收集,PS 域包含一个独立的功能称为 CGW(计费网关)。CGW 收集来自 PS 域单元的计费数据,并把这些数据转发到计费中心进行后处理。计费也是一些 GRX 漫游配置中考虑的主要因素。一种典型的情形是,当用户访问兼容 GPRS 的网络时,用户的归属网络就会安排一个 GGSN 用于 GPRS 连接。此时,归属网络的运营商负责收集与该 GPRS 连接相关的计费信息。这种配置就要放弃对归属运营商的 APN 的控制。根据前面对 APN 的说明,这个"归属网络 GGSN"配置不允许使用万能 APN,如果漫游中使用了拜访网络的 GGSN,就要允许万能 APN。

如图 6.7 所示,PS 域维护着不同的连接。首先,它维护指向接入网的 Iu_{PS} 接口,UTRAN 和 GERAN 通过这个接口连接。当 GERAN 以这种方式连接到网络中时,称该

网络使用了"GERAN Iu 模式"。GERAN 连接还可能使用基于帧中继的 Gb 接口，此时称为"GERAN Gb 模式"。在 PS 域连接时，UTRAN 只能采用 Iu 接口。可能的补充接入方式及其互连机制仍在研究之中。

其次，PS 域有一个到 CN 公共功能实体（如 HSS、EIR）的连接。PS 域通过这些连接处理 6.1.1 节所述的任务。

对于 IMS 支持的成熟多媒体业务来说，PS 域是一个网络平台。因此 PS 域包括到 IMS 的接口。IMS 及其结构将在 6.4 节讲述。

6.2 核心网管理任务和控制任务

前一节简述了核心网的体系结构问题，本节稍有不同，我们将从管理和控制的角度来研究 CN 的作用。

如图 6.8 所示，就 CM（通信管理）而言，主要的两个任务就是连接管理和会话管理。连接管理负责 CS 事务及相关事项的管理任务，而会话管理可认为是连接管理在网络的 PS 端的对应物。CM 信息处理呼叫和会话控制，携带 CM 信息的一组控制协议称为"COMC（Communication Control，通信控制）协议"。

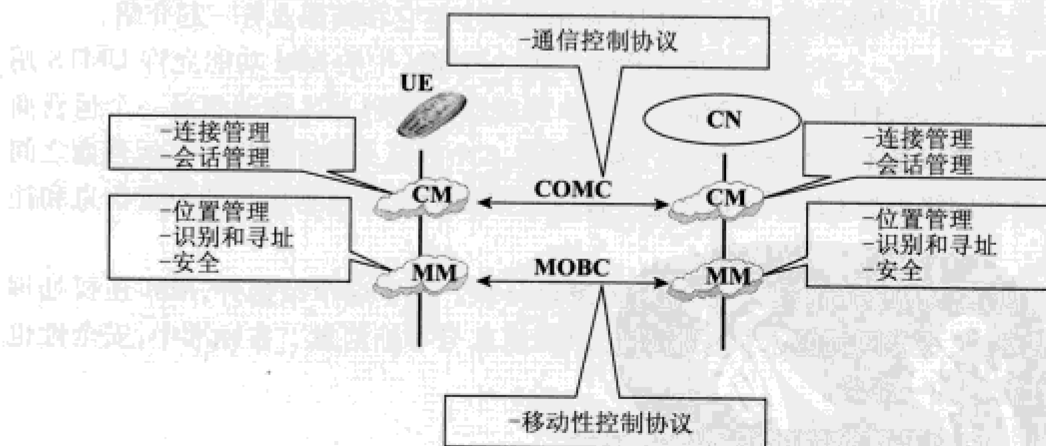


图 6.8 核心网管理任务和控制任务

MM 的任务包括 UE 位置管理以及相关的身份识别和寻址，MM 管理任务也包括其他相关事项，如安全性也是 MM 的一部分。安全性将在第 9 章详细介绍。支持 MM 任务执行的控制协议请参考 MOBC（Mobility Control，移动控制）协议。

6.2.1 移动性管理

这里要讲的是世界范围内 2G 蜂窝网络中的移动性。对移动性的本质理解使移动网络设计与固定通信出现了明显差别，尽管更加复杂，它为终端用户创造了大量全新的潜在业务种类。

我们首先看与用户移动性相关的两个基本概念的区别。

- 位置(location)。
- 定位(position)。

"位置"是指终端用户(及其终端)在网络的逻辑结构中所处的位置。在这种逻辑结构中可识别的单元是小区或者由多个小区组成的区域。注意"区域"不一定指一组地理位置相邻的小区,它是网络运营上根据网络操作的需要使用的词汇。

另一方面,"定位"则是指网络覆盖区域中终端用户(及其终端)的地理位置,它由一对标准的坐标值给定。在最基本的情形中,如果没有进行地理定位,那么定位信息可由小区标识码得到,例如就是控制该小区的 BS 的地理坐标。

尽管位置和地理定位都可以说明用户在哪里,但 UMTS 中使用这两个词汇的方式完全不同。位置信息用于网络连接到有激活通信的用户。地理定位信息则是当一些外部业务(如急救呼叫中心)提出请求时,才由 UMTS 网络给出。地理定位信息对急救呼叫是"性命攸关"的事情,而位置信息对网络向移动用户提供业务也是"性命攸关的"。

地理定位的主要目的是支持面向应用的业务,当然网络内部也可以利用地理定位信息,如地理定位辅助的切换和网络规化的优化等。

移动定位是一种提供的业务,我们将在第 8 章中将它和其他业务一起介绍。

MM 产业的另一个关键业务就是漫游。单一 PLMN 中的 MM 功能允许 UMTS 用户在其覆盖区域内自由移动。漫游也使用户可以从一个 PLMN 移动到另一个运营商的网络,甚至可以是不同国家的网络。为了漫游,CN 中定义的许多接口是运营商之间的接口,拜访网络中的 CN 单元通过这些接口从归属网络中得到用户的位置信息和注册信息。

如前所述,MM 运行需要一种相对的逻辑分级。除了这个结构外,MM 还要处理用户及其终端、相关网元的永久或临时的识别信息与寻址信息。在标准中,安全性也是移动性管理的一部分。

6.2.1.1 用户及其终端的识别码和地址

和固定网络不同,UMTS 网络需要使用多种编号和识别码以用于不同的目的。顾名思义,在固定网络中用户和设备的位置是固定的,这样与此相关的许多事情都是恒定不变的。如果用户的位置不再固定,固定的编号方式也就不再有效。UMTS 使用的不同识别码的目的可总结如下。

- 唯一识别码:为用户提供一个全球唯一的识别码。对于所有存储有用户信息的寄存器来说,这个识别码是搜索时的主要关键词,它也是计费的依据。
- 业务分离:尤其在移动台被叫的通信中,必须能识别出将要使用的业务。这一点是通过使用一个和用户唯一识别码有关的识别码来实现的。
- 路由目的:某些特殊情况下需要执行路由功能,它对任何网络和国界都不是固定的。

● 安全性：蜂窝环境中的安全性是一个非常重要的问题，因此需要产生其他识别码来保护用户的隐私。这些与安全相关的识别码是可选的，但还是强烈推荐使用。

6.2.1.1.1 国际移动用户识别码

移动用户的唯一识别码称为 IMSI（International Mobile Subscriber Identity，国际移动用户识别码）。IMSI 由三部分组成：

$$IMSI = MCC + MNC + MSN$$

其中，MCC 是移动台国家码（3 位数字），MNC 是移动网络码（2～3 位数字），MSN 是移动用户编号（9～10 位数字）。这个编号存储在 SIM 卡（USIM）中。在 HLR、VLR、AuC 和 SGSN 中，IMSI 起着唯一的数据库搜索关键字的作用。其编号规则遵循 ITU-T 的 E.214 标准。当移动用户漫游出归属网络时，访问服务网络向 UE 发出请求，要求 UE 提供这个编号，从而能识别出用户的归属网络。对于用户归属网络的 HLR，IMSI 是唯一的数据库搜索关键字，因此按 IMSI 提出请求时，HLR 能够返回用户的描述文件及其他信息。归属网络中的安全信息请求也是这样一个过程，如图 6.9 所示。

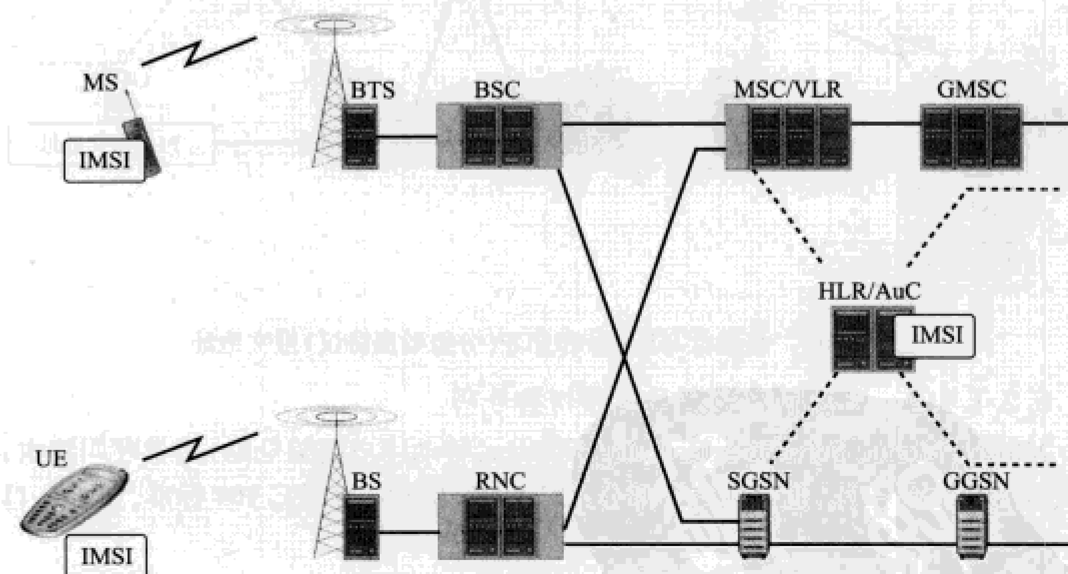


图 6.9 国际移动用户识别码

6.2.1.1.2 移动用户 ISDN 号及 PDP 报文地址

IMSI 用于真正的用户识别。而 MSISDN（Mobile Subscriber ISDN Number，移动用户 ISDN 号）用于业务分离。这是因为一个用户可以有多个激活的业务，靠 MSISDN 来区分它们。例如一个移动用户可以有一个 MSISDN 号用于语音业务，另一个 MSISDN 号用于传真等。移动台主叫的通信连接不需要 MSISDN，因为通信连接时的 CM 消息中有业务指示。移动台被叫时需要不同的 MSISDN 用于不同的业务，因为周围的网络不一定能通过其他方式提供业务信息。MSISDN 由三部分组成：

$$MSISDN = CC + NDC + SN$$

其中，CC 是国家码（1～3 位数字），NDC 是国内地区码（1～3 位数字），SN 是用户编号，编

号格式遵循 ITU-T 的 E.164 标准。经常把这个号码称为“目录号”或者“用户号”。

PS 中与 MSISDN 对应的是 PDP(分组数据协议)报文地址,即移动用户的 IP 地址。PDP 报文地址可以是动态的或静态的。动态地址在产生分组会话时建立,静态地址由 HLR 定义。静态的 PDP 报文地址和 CS 中的 MSISDN 类似,如图 6.10 所示。

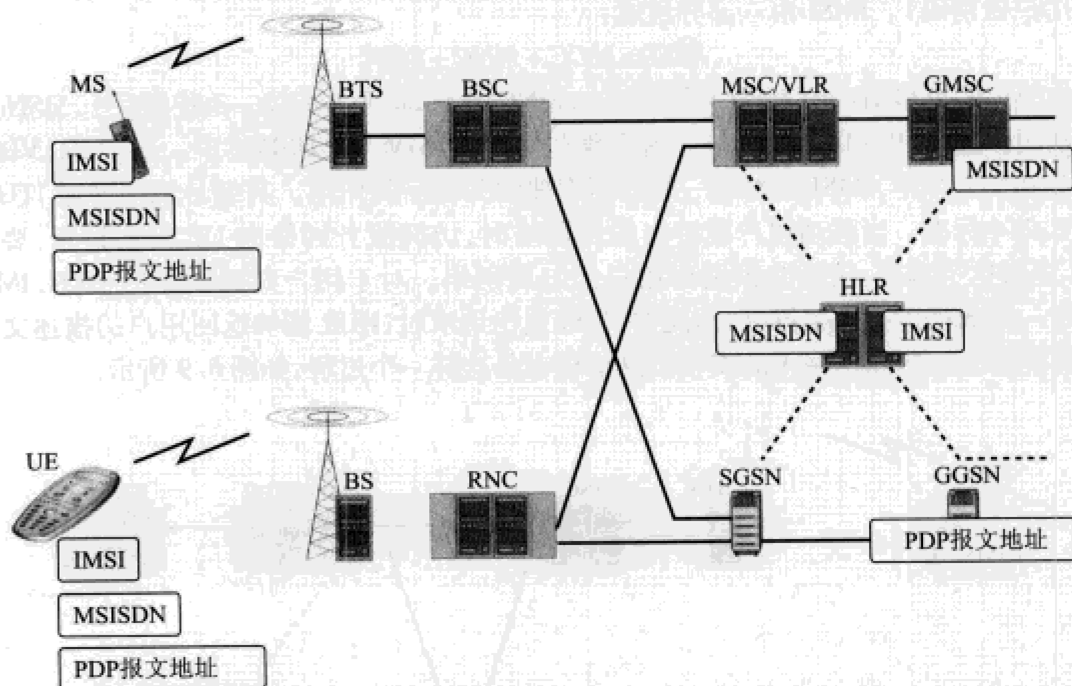


图 6.10 移动台 ISDN 号和 PDP(分组数据协议)报文地址

6.2.1.1.3 移动用户漫游号码和切换号码

MSRN(Mobile Subscriber Roaming Number,移动用户漫游号码)用于呼叫路由,其格式和 MSISDN 一样,也包括三个部分:CC、NDC 和 SN,遵循 E.164 标准,如图 6.11所示。

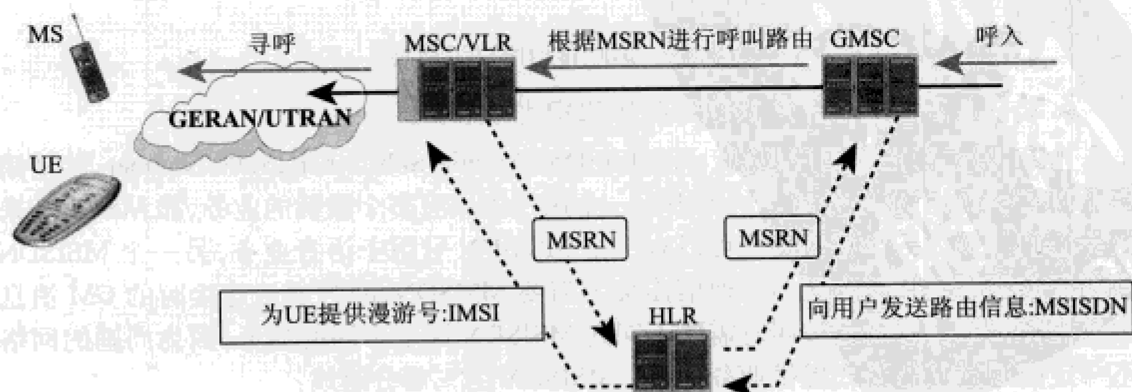


图 6.11 MSRN

MSRN 用于 GMSC 和服务 MSC/VLR 之间，移动台被叫的通路连接中，所分配的 MSRN 号能够识别国家、网络以及网络中的网元。MSRN 中的用户部分用于识别用户。在 MSC 到 MSC 的切换中，MSRN 用于两个 MSC/VLR 之间的呼叫通路连接。此时的 MSRN 通常也称为 HON(Handover Number，切换号码)。

6.2.1.1.4　临时移动用户识别码及 P-TMSI

出于安全性考虑，唯一识别码 IMSI 应尽量不要以明文方式传输，这一点非常重要。所以，UMTS 用 TMSI(Temporary Mobile Subscriber Identity Number，临时移动用户识别码)来代替原来的 IMSI。CN 中 PS 域也有类似的临时识别码，称为 P-TMSI (Packet Temporary Mobile Subscriber Identity，分组临时移动用户识别码)，以区别于 TMSI。

TMSI 和 P-TMSI 都是随机格式的编号，它们有限定的有效期和有效范围。TMSI 由 VLR 分配，其有效期持续到 UE 开始下一次通信，如图 6.12 所示。P-TMSI 由 SGSN 分配，在 SGSN 范围内有效。每当 UE 更新路由区时，P-TMSI 也随之改变。

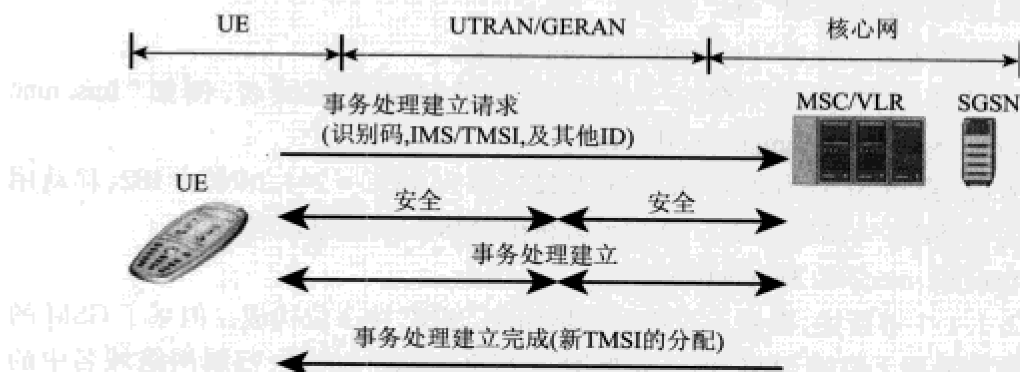


图 6.12　TMSI 的分配

6.2.1.1.5　国际移动设备识别码

出于移动设备识别的目的，定义了两种稍有区别的编号：IMEI(International Mobile Equipment Identity，国际移动设备识别码)及其扩展：IMEISV(International Mobile Equipment Identity and Soft Version，国际移动设备识别软件版本号)。这些号码由 EIR (Equipment Identity Register，设备识别寄存器)处理。它们的网络处理流程也类似：UE 根据具体要求提供某一种号码，网络通过 EIR 核查该号码的状态。号码结构如图 6.13 和图 6.14 所示。

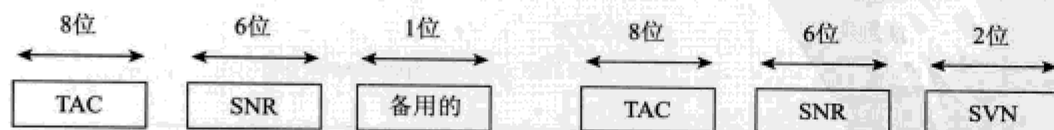


图 6.13　国际移动设备识别码(IMEI)　　图 6.14　国际移动设备标识软件版本号(IMEISV)

这两种编号的共同点是,TAC(型号分配码)定义制造商和话机型号,同一TAC下的一件设备对应唯一的SNR(序列号)。IMEI定义的长度为15位,剩下的一位为空。UE向网络发送IMEI时把这一位填上0。网络取IMEI的高14位,并计算校验位的值以确定传输过程的正确性。

IMEISV比IMEI多两位,表示硬件的软件版本号。允许UE发送IMEI或发送IMEISV,但不可以同时发送两个号码。

注意IMEI是硬件的唯一标识,它始终不变,而在IMEISV中的SVN部分会因软件升级而改变。软件升级后IMEISV的其他部分不变。

6.2.1.1.6 IMS——归属网络域名

IMS归属网络域名遵循因特网上的域名结构,只是包括了移动网络特定的部分。为了使移动网络和因特网有不同的域名空间,IMS归属网络域名包含了IMSI号的一部分。

用户确定归属网络域名时包括以下一些步骤。

①根据IMSI确定出MNC和MCC。

②归属网络域名总是以“ims”开始。

③归属网络域名总是以“3gppnetwork.org”结束。

④以上第②步和第③步合在一起就形成了归属网络域名,例如“ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org”。

举例来说,若IMSI号为244 182 123123123,那么MCC=244,MNC=182,移动用户识别码为(MSIN)=123123123。这样可解析出IMS归属网络域名为:

ims.mnc182.mcc244.3gppnetwork.org

如6.2.1.1.1节所述,在基于UMTS的网络中,MNC由3位构成。但基于GSM的网络大多数都采用2位的MNC值。如果网络MNC是2位的话,归属网络域名中的MNC前面应补一个“0”。

6.2.1.1.7 IMS——私有用户识别码

IMS的运行需要私有用户识别码。这些识别码遵循因特网的使名结构:username@realm。私有用户名原则上可以是任意的,但UMTS用户名实际上是从IMSI中导出的,因为IMSI就是一个很好的私有用户标识码,并且是唯一的。

对于前例中的IMSI号,私有用户识别码构成如下。

IMSI	244 182 123123123
MCC	244
MNC	182
MSIN	123123123
域	ims.mnc 182.mcc244.3ppnetwork.org
用户名	IMSI

根据这些值,本例中的私有用户识别码为:

244182123123123@ims.mnc 182.mcc244.3gppnetwork.org

私有用户识别码很像 IMSI,其作用也有部分相似。它存储在 ISIM(IMS 识别模块)中,有如下一些主要的特点。

- 它包含于所有 UE 向网络(IMS)发出的注册请求中。
- IMS 有私有用户识别码的注册和取消注册状态。
- 只要用户有效,它就是有效和固定不变的。
- 在任何情况下,UE 都不能修改其私有用户识别码。
- HSS 存储私有用户识别码。

6.2.1.1.8 IMS——公共用户识别码

私有用户标识码用于网络内部,为了能访问用户,还需要有公共用户识别码。这是因为当我们谈及一个移动用户的时候,应能用因特网的地址方式通过因特网访问,并能者用 E.164 MSISDN 号按传统的移动设备访问。

因特网方式的公共用户识别码就是 SIP URI,其格式是:

sip:firstname.lastname@operator.com

电话式的公共用户识别码根据前述的标准 MSISDN 号定义。比如 MSISDN 号为 +358 661 231 234,那么按 Tel URL 表示就是:

tel:+358661231234

也有可能需要指示出 Tel URL 所依据的编号规划。上例给出的是全球编号规划。如果采用本地编号规划(可能没有国家码和网络码),那么 Tel URL 中应指示出号码规划的范围和所有者。

公共用户标识码有以下几个主要特点。

- 两种格式中的一种:SIP URI 或 Tel URL。
- 至少有一个公共用户识别码存储在 ISIM 中。
- 使用 IMS 会话和业务之前必须先注册。

一个用户可以有多个公共用户识别码。

6.2.1.2 定位结构及其标识

除了用户及其终端的地址和标识码外,MM 还要求网络具有逻辑结构,如图 6.15 所示。这个结构代表接入网络的逻辑部分。它就像 MM 处理过程和参数配置时所用的一张“地图”。UMTS 基本上包括 4 个逻辑定义。

- LA(Location Area,位置区)。
- RA(Routing Area,路由区)。
- URA(UTRAN Registration Area,UTRAN 注册区)。
- 小区。

在 CN CS 域中,LA 是 UE 可以自由移动而无需进行位置更新的区域。LA 由小区组成,最小为 1 个小区,最大为 VLR 中的所有小区。位置更新过程使 VLR 以 LA 的精确度更新 UE 的位置。移动台被叫时需要这一信息。为了得到这一信息,VLR 在目标 UE 最后一次进行位置更新所在的 LA 内对其进行寻呼。

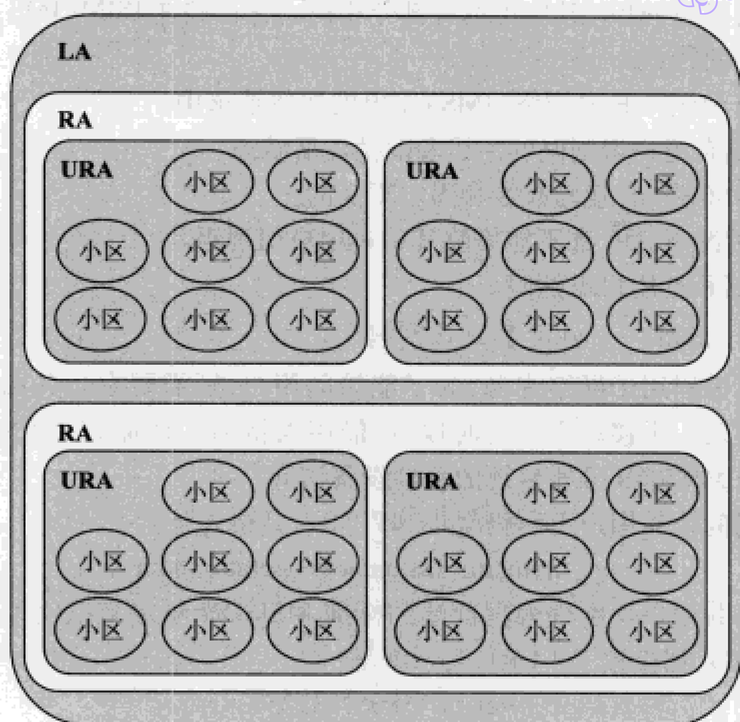


图 6.15 MM 的逻辑实体及其关系

需要注意的除 VLR 之外,在其他方面,LA 没有硬件限制。例如,一个 RNC 可以有多个 LA,一个 LA 也可以覆盖多个 RNC。每个位置区都通过 LAI(Location Area Identity,位置区识别码)唯一标识。LAI 由以下几部分组成:

$$LAI = MCC + MNC + LA\text{ 码}$$

其中的 MCC 和 MNC 与 IMSI 号中的格式相同。LA 码就是标识 LA 的编号。LAI 是全球唯一的编号,在相同网络中显然不能出现相同的 LA 码,因为一个 VLR 不能处理两个重复的 LA 码。UE 从广播信道 BCH 侦听 LAI,其内容与具体的小区有关,由 RNC 决定。

和 CN CS 域一样,PS 域根据 RA 进行位置注册过程。RA 和 LA 非常相似,UE 在这个区域内移动时无需进行 RA 更新。另一方面,RA 是 LA 的"子集":一个 LA 可以有多个 RA,但反过来不成立。另外,一个 RA 不能属于两个 LA。

在 CS 的 VLR 和 PS 的 SGSN 之间有一个可选接口 Gs,通过这个接口,它们可以交换位置信息。由于 UMTS 必须能与 GSM 互通,所以 UMTS CN 也支持 GSM 的特性。其中之一就是组合 LA/RA 更新,GSM 终端执行更新请求,并在第一位置发向 SGSN。如果有可选的 Gs 接口,那么 SGSN 也可以使用这接口来请求 VLR 对 LA 注册进行更新。普通 UMTS 网络中没有这个选项,因此不能进行组合成 LA/RA 更新,UE 只能在 CN 的两个域内分别注册其位置。

在 GSM 网络中,MM 完全在终端和 NSS 之间处理。在 UMTS 中,UTRAN 部分介

入了 MM,因此有了一个局部的移动性注册,即 URA(UTRAN Registration Area,UTRAN 注册区),在第 5 章已讨论过。这一点看上去很小,但它对 SGSN 的内部结构带来了巨大的变化,它使 3G SGSN 实际包含了 2G SGSN 和 3G SGSN 的功能。在 UMTS 中,SGSN 根据 URA 识别码承载到 UE 的隧道 IP 业务;而在 2G 中,隧道 IP 业务在 SGSN 处中止,然后通过 2G 特有的 Gb 链路进行中继。

因为 URA 与 LA 或 RA 的定义非常相似,所以在网元这个层面上说,原则上对它在没有任何限制。但在实际当中,URA 和 RNS(无线网络子系统)之间的关系或多或少是固定的。从另一方面说,URA 是一种逻辑定义,它结合了业务路由和 RRC(无线资源控制)。在路由中,URA 寻址实体指向接入域;在 RRC 中,终端的状态指示出位置精度和业务接收能力。这一点可见第 5 章中简要介绍的 RRC 状态模型。

MM 逻辑实体中最小的"模块"是小区。CN 基本上不需要直接识别小区,只需识别小区集合。接入域的小区是具有公共识别码的最小实体,称为 CI(Cell ID,小区识别码)。如同 LA 码,CI 是一个网内唯一的编号。为了能全球区分小区,需对其进行扩展,称为 CGI(Cell Global Identity,小区全球识别码)。CGI 格式如下:

$$CGI = MNC + MCC + LA\text{ 码} + CI$$

CGI 的值包括网络所在国家(MCC)、国内的网络(MNC)、网络的 LA 以及小区在网络中的编号。这个信息由 UTRAN 的系统信息广播功能发布给 UE。

6.2.1.3 CN 和接入网公用的网络级识别码

本节简要介绍一些通过 Iu 接口传输的识别码,它们对 CN 和 UTRAN 都是公用的。其中有些也用于与其他网络的互连。

如图 6.16 所示,每一个 PLMN 都有其自己唯一的 ID 值。名为 PLMN-id。它由两个参数构成:MCC 和 MNC,它们和 IMSI 所用的同名参数等价。

$$\text{PLMN-id} = \text{MCC} + \text{MNC}$$

PLMN-id 是网间传输时非常方便的全球唯一标识,因此可以有许多用途。例如 CGI 和 LAI 都是以 PLMN-id 开头的。

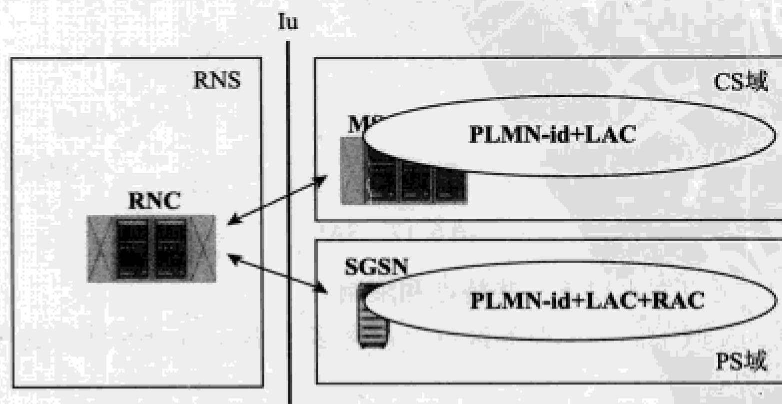


图 6.16 核心网域的识别码

网内的 RNS 必须能定位出维护 Iu 接口的 CN 域边缘节点，为此需要用 CN 域标识码。当 Iu 接口上建立了链接并且 SRNS（服务 RNS）功能被重定位（即 Iu 接口上的承载发生变化，需要用另外一个 RNS）时，就需要 CN 边缘域信息。

CN CS 域标识码由 PLMN-id 和 LAC（位置区码）组成，CN PS 域标识码则包含 PLMN-id、LAC 和 RAC（路由区码）。

在 CN 内部，可能需要对其单元进行全球标识。为此可以使用 CN-id（CN 标识码）。这也对每个网络中 CN 单元的个数设立了理论上的极限。CN-id 由两个值构成：PLMN-id 和一个 0～4 095 之间的整数：

全球 *CN-id* = *PLMN-id* + <0…4 095>

注意此标识码不是网络单元的地址。CN-id 是一个全球唯一的序号，另外 CN 中的单元并非都有 MSISDN 类型的地址用于 SCCP（信令连接控制部分）的路由目的。

RNC-id（RNC 标识码）的格式和 CN-id 完全相同，用于 RNC 单元和 BSC（若 GERAN 采用 Iu 模式）。

全球 *RNC-id* = *PLMN-id* + <0…4 095>

SAI（业务区标识码）标识同一 LA 中的一个或多个小区组成的区域，可被所有 CN 域识别。可用来向 CN 域指示 UE 的位置。图 6.17 是 SAI 的示例。

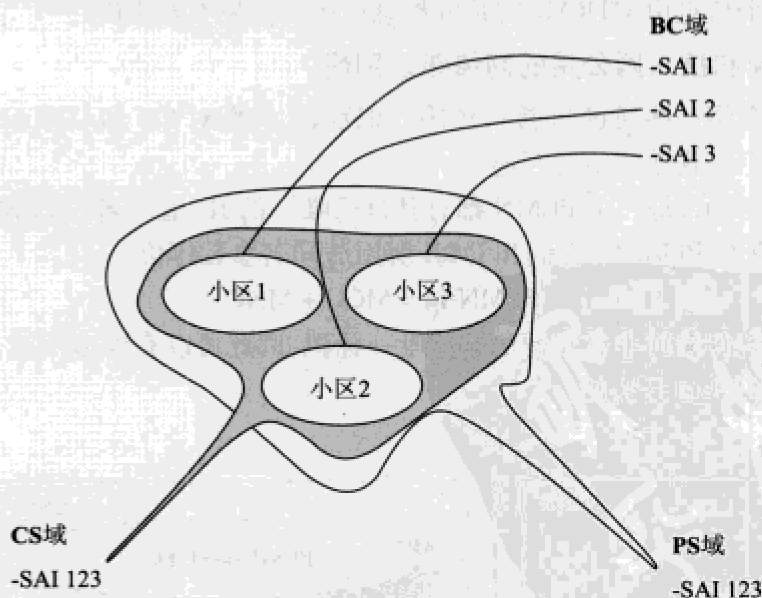


图 6.17 SAI

通过图 6.17 可以发现以下一些特点和限制。

- PS 域和 CS 域中的一个业务区可以包含多个小区，而 BS 域中的一个业务区只有一个小区。
- 一个小区最多可定义两个 SAI。此时一个用在 CS 和 PS 域，另一个用在 BC 域。
- SAI 的格式为 *PLMN-id* + *LAC* + *SAC*，其中 SAC 代表业务区码。

由于许可及实现成本的原因，网络共享的商业需求还在许多国家的讨论之中。实际上，网络共享是目前修订中的3GPP R6标准的一个议题。一个网络可以有多中共享方式，但是如果实现了共享，就必须能识别出网络中所共享的部分。为此，目前已经引入了SNAI(共享网络区域标识别码)。

SNA(共享网络区)由LA构成，后者将被重新定义为SNA。在此区域中的UE可以接入不同运营商的网络。SNAI或SNA-id包含PLMN-id和共享网络区域码(SNAC)：

$$SAN\text{-}id = PLMN\text{-}id + SNAC$$

SNA-id包含了PLMN-id，因此它是全球唯一的。

6.2.1.4 移动性管理状态模型

分组连接及其管理对MM带来了新的问题，因为分组连接中MM有一个状态模型。CS连接中基本上也存在同样的模型，但不经常使用，因为CS连接行为并不需要此类状态模型。如图6.18中所示，缩写词MM指CSMM，而PMM指PS MM。

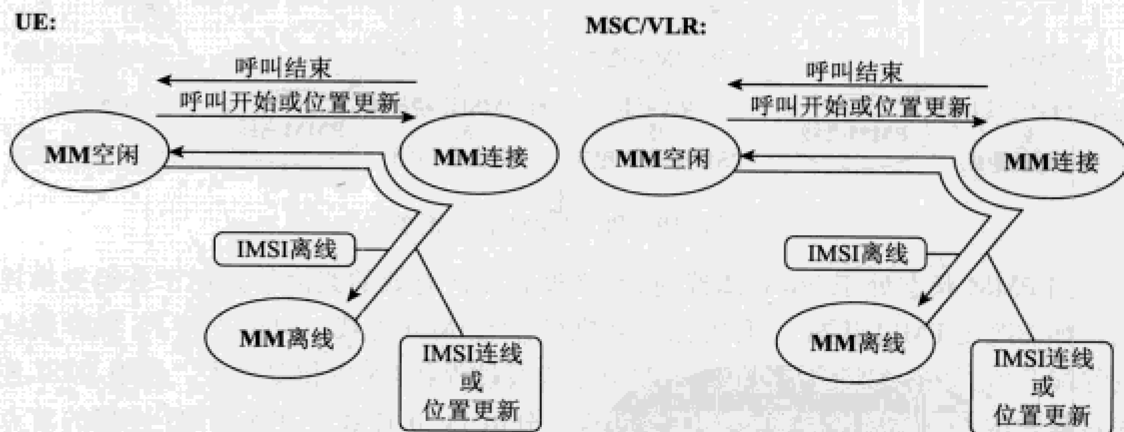


图6.18 CS(电路交换)MM(移动性管理)状态模型

6.2.1.4.1 电路交换模式的MM状态

从移动管理的角度来说，终端的网络连接有3种状态：MM离线、MM空闲和MM连接(MM-detached、MM-idle和MM-connected)。这些MM状态表示了终端位置在图6.15逻辑结构下的准确程度。在MM离线(关机)状态，网络无从知道终端/用户的位置。在MM空闲状态，网络能知道终端在哪个LA。在MM连接状态，能知道在哪个小区。

图6.18所示的情形对GSM NSS(Network SubSystem，网络子系统)和UMTS CS域(3GPP R99之后)都是类似的。当用户开机时，终端将执行IMSI连线或位置更新过程。当用户关机时，MM状态就从MM闲置变为MM离线。如果从驻留小区识别出来的LAI与终端存储在USIM上的相同，就执行IMSI连线。如果不同，则执行位置更新，以注册它的新位置。无论是哪种情况，MM状态变化都是：MM离线—MM连接—

MM 空闲。这里要说明的是,终端执行这些过程时,网络偶尔能知道终端在小区精度的位置。这两个过程通过发送包含原小区信息和事务原因的消息"唤醒"CS 域。在 GSM 中,这个消息称为 CM 业务请求(CM Service Request),在 UMTS 中则称为 UE 初始消息(UE Initial Message)。

当用户激活(MM 空闲,终端开机)时,MM 状态按照终端的使用情况在 MM 空闲和 MM 连接状态之间变换。简单地说,当一个呼叫开始时,MM 状态从 MM 空闲状态变到 MM 连接状态,当呼叫结束时,MM 状态又从 MM 连接状态转变到 MM 空闲。

6.2.1.4.2　分组交换模式的 MM 状态

从 PMM 来说,分组交换连接的情况有所不同:PMM(Packet Mobility Management,分组移动性管理)的状态还是一样的,但是触发状态转移的原因不同(见图 6.19)。

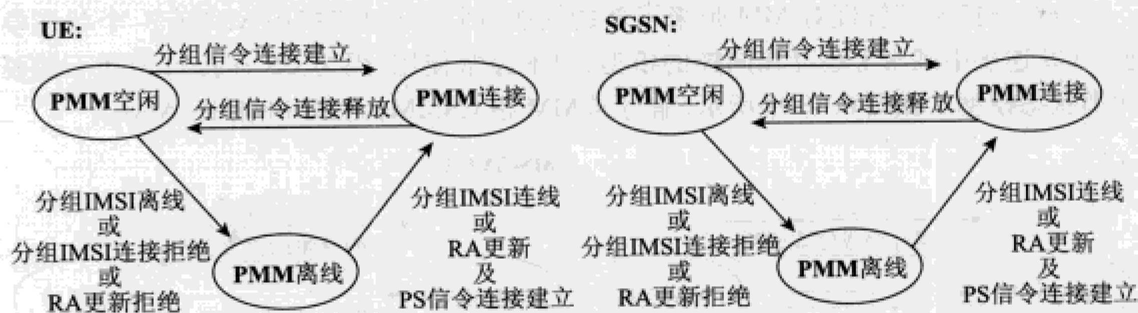


图 6.19　PS 的 MM 状态模型

当 PMM 状态处于 PMM 离线时,网络没有任何有效的路由信息用于分组交换连接。如需改变 PMM 状态,一种方法就是执行分组 IMSI 连线。只要支持 PS 操作模式的终端开机,就会产生这个过程。不过分组连线过程和 CS 中相差很大。分组 IMSI 连线过程和位置更新相比有更多的信令过程。分组 IMSI 连线要在所有 PS 连接的节点上建立有效的路由信息,包括 SGSN 和 GGSN。此外还需要请求从 HLR 中获得用户描述数据,并可能需要取消旧的路由信息。

在 PMM 连接状态,数据可以在终端和网络之间传输:SGSN 知道分组传输的有效路由信息,能确切到实际 SRNC 的路由地址。在 PMM 空闲状态,位置信息能确切到 RA 标识码。在 PMM 空闲状态,为了能联系到终端(如为了传输信令),需要有寻呼过程。

从终端用户角度看,分组交换移动连接通常被看成是"永远在线",而从另一方面来看,每一次分组呼叫又可以说成是很多短小的电路交换呼叫。这两种说法都有道理,但不完全对。从网络的角度看,PS 移动连接产生了"永远在线"的幻觉,它是 PMM 连接和 PMM 空闲状态产生的。在 PMM 空闲状态,网络和终端都有有效的路由信息,并已准备好传输分组数据,但它们并不能在这个状态下进行传输,因为接入网中没有连接。

当用户关机时,MM 返回到 PMM 离线状态,网络节点中可能存在的路由信息不再有效。如果出于某种原因,分组 IMSI 连线或者 RA 更新出错,MM 状态也返回到 PMM 离线。

6.2.2 通信管理

本小节简述 CS 和 PS 通信方面主要的 CM(通信管理)功能。这个功能在 CS 方面称为 CM,在 PS 方面称为会话管理(SM)。本节的简述将包括连接的阶段、会话管理处理过程以及相关的实体。

6.2.2.1 电路交换连接管理

连接管理是描述交换机中呼入和呼出事务处理所需功能的高端名称。一般来说,在 CS 通信连接之前,交换机先要做三件事情:号码分析、路由和计费。连接管理可分为三个功能阶段,实现完全连接必须经过这三个阶段(见图 6.20)。

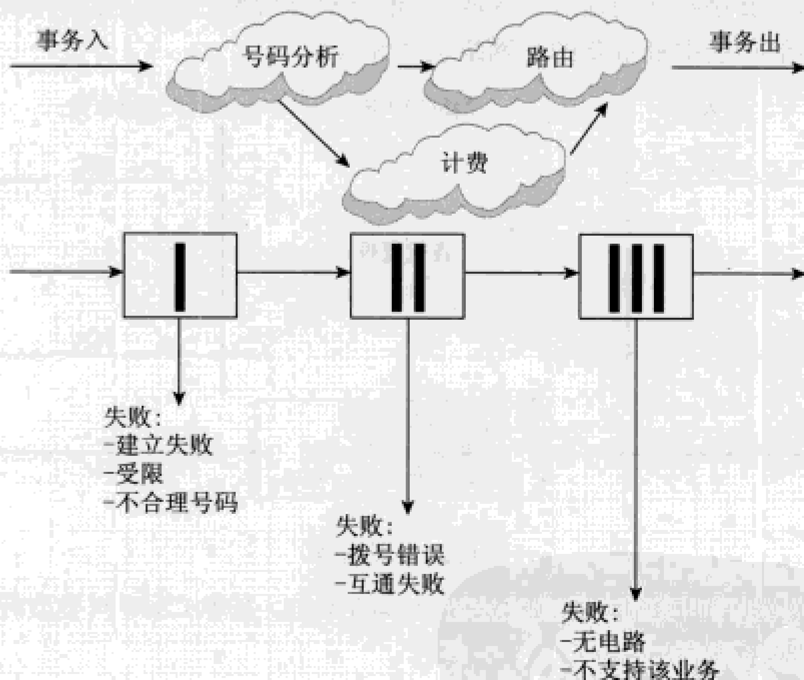


图 6.20 电路交换连接管理——连接图

号码分析是处理到达事务的一些规则。发起事务的用户号码称为主叫号码,事务所欲连接的号码称为被叫号码。号码分析根据预订的规则对这两个号码进行分析,并做出相应的决策。在连接管理阶段 I 和阶段 II 都要进行号码分析。在阶段 I,交换机检查被叫号码是否合理,是否对该主叫有呼入屏蔽之类的限定。

在阶段 II 中,系统主要关注被叫号码。根据事务的性质确定该呼叫是国际呼叫还是国内呼叫,该被叫是否有已定义的路由规则?此外,系统还要检查该事物是否要求连接互通设备(如调制解调器),是否需要计费。该事务的统计工作也在这一阶段开始。

连接管理阶段 II 成功后,系统就知道了事务欲连接到什么地方。这个连接以及和信道选择过程称为路由。根据正确的事务目的地,系统开始通过 ISUP(ISDN User Part)等信令协议建立通向目的地的信道/带宽。在事务进行中,交换机存储有关事务

即其连接的统计信息；如果该事务是需要计费的，它还要收集计费信息。当事务结束时，连接管理阶段Ⅲ负责释放相关的资源。

在固网中，两端都把每个呼叫视为一个实体。在蜂窝网络中，"呼叫"一词可以有许多解释。每一个"呼叫"都是由若干个呼叫臂组成的，每个臂都是呼叫的一部分。

从连接管理的角度来看，每一个呼叫至少由两个呼叫臂构成。这里有4种可用的臂：MOC（Mobile Originated Call，移动台主叫）、MTC（Mobile Terminated Call，移动台被叫）、POC（PSTN Originated Call，PSTN 主叫），PTC（PSTN Terminated Call，PSTN 被叫）。如图6.21所示，连接管理实际上是一个分布式功能，根据不同单元使用呼叫控制的不同部分。服务 MSC/VLR 处理 MOC 和 MTC 呼叫臂，GMSC 处理 POC 和 PTC 臂。呼叫控制能够接收和创建这些呼叫臂，也能根据臂和呼叫的类型判断是否还需要其他功能。其他功能中最重要的是网络互通和计费。

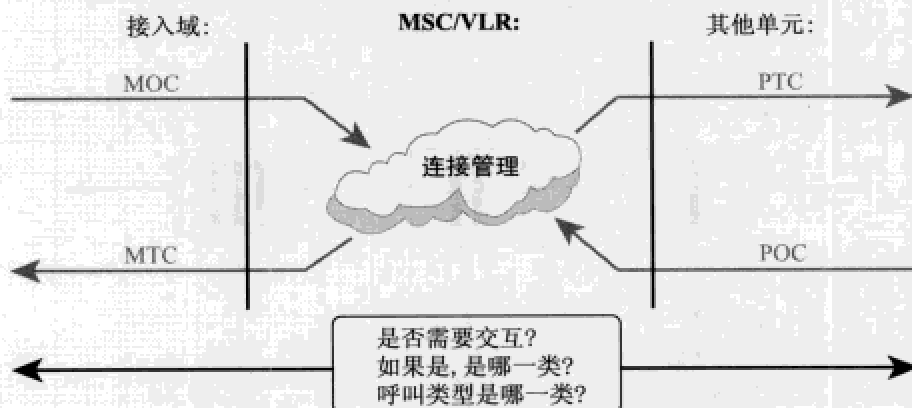


图6.21 呼叫臂

呼叫控制识别呼叫类型并据此决定进一步的操作。基本 CS 呼叫类型有如下几种。

- 正常呼叫（语音）。
- 紧急呼叫。
- 数据呼叫（包括传真）。

MOC 臂的呼叫类型包含在"CM 业务请求消息"和"UE 初始消息"中。POC 臂的呼叫类型"隐藏"在被叫方地址。正如 MM 中所述，所用业务是被叫方根据 MSISDN 号识别的。在 MTC 和 PTC 臂中，连接管理判断呼叫臂之间是否需要某种交互。

6.2.2.2 分组通信的会话管理

在 PS 域中，分组连接称为会话，它们由 SM（Session Management，会话管理）实体建立和管理。

SM 是一个逻辑实体，它有两种主要状态，未激活和激活，如图6.22所示。在未激活状态，分组数据不可能传输，路由信息即便有也是无效的。在激活状态，可以传输分组数据，存在有效的路由信息并且已定义。

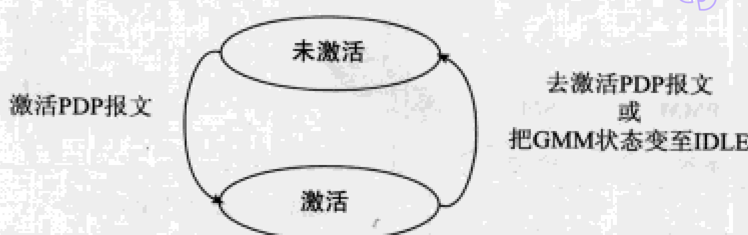


图 6.22 SM(会话管理)状态模型

在激活会话期间用于分组数据传输的协议是 PDP(Packet Data Protocol,分组数据协议)。CN PS 域的设计允许使用多种 PDP 协议。最显然的情形是使用 IP 协议作为 PDP 协议,但也支持 X.25 等其他协议,后一情形比较少见。

SM 把分组任务属性按报文处理,称为 PDP 报文。PDP 报文通过端点地址和 QoS 包括了所有描述分组数据连接的参数。例如 PDP 报文有这样一些信息,如分配的 IP 地址、连接类型以及相关的网元地址。当 SM 激活时(即存在 PDP 内容),用户也有一个 IP 地址。从业务的角度来看,每个有一定 QoS 等级的 PS 业务建立有一个 PDP 报文。因此,分组连接的网页浏览和视频流媒体等各有其 PDP 报文。

根据定义,UMTS 采用下面的 QoS 等级。

- 会话级别(conversational class)。
- 流媒体级别(streaming class)。
- 交互级别(interactive class)。
- 背景级别(background class)。

第 8 章中将对它们进行了更详细的讨论。

PDP 报文在 UE 和 GGSN 中都有定义,并包括所有关于分组连接特性的相关参数。PDP 报文可以是激活的、去激活的或者修正的。

激活 PDP 报文将使 SM 从非激活状态变成激活状态。SM 的这一状态改变也就意味着 UE 形成了一个分组会话,网络拥有有效的分配地址信息,并且分组连接的特性也已定义(如所用的 QoS)。当 PDP 报文被激活时,UE 和网络就可以建立用于数据传输的承载。

去激活 PDP 报文将使 SM 的状态变为未激活。此时,UE 和网络可能有的地址信息和分组会话信息不再有效,UE 和网络也因此不能建立任何连接以传输用户数据流。

当 SM 处于激活状态且 PDP 报文存在时,PDP 报文可以被修改。UE 和网络在修改过程中重新协商分组会话的特性。典型的协商议题是分组会话的 QoS 等级。

如图 6.23 所示,SM 为高级别的实体,它的活动依靠低级别的实体,如 PMM 和 RRC。如果 RRC 和 PMM 的状态不适合激活的分组会话,那么 PDP 报文将被去激活,SM 的状态将从激活转为未激活。例如当 RRC 从连接状态变为空闲状态时就会出现这样的情形。这一状态变化将触发 PMM 从连接状态变为空闲状态,如果考虑图 6.22 所示的 SM 状态模型,那么 PMM 状态的改变将进一步触发 SM 的状态从激活转变为未激活。

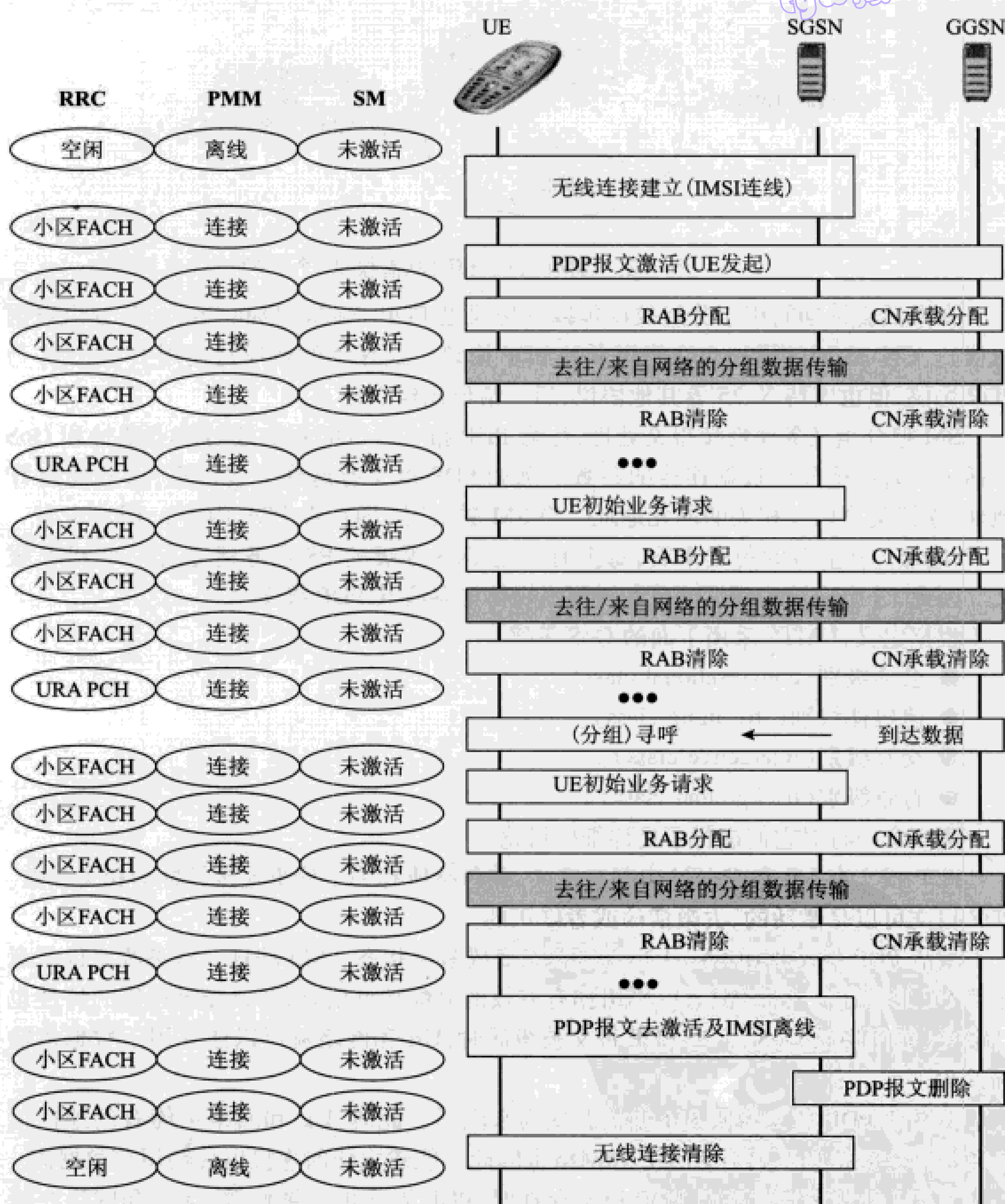


图6.23　在分组流期间的RRC(无线资源控制)、PMM(分组移动性管理)及SM的状态示例

SM的目的是为终端用户建立一种持续连接的感觉,并且必须要以一种有效的方式实现以尽量节约网络资源。例如,当有请求时,就建立RAB以携带用户数据,而当没有数据要传时,就清除RAB,但继续保留分组信令连接。图6.23示出了一个分组数据流期间,CN和UTRAN中不同的管理和控制实体的状态变化。在这个实例中,用户

开机后进行 IMSI 连线。然后用户向网络发送分组数据。业务提供商也向终端发送分组数据。这个过程重复进行,过了一段时间后,网络向 UE 发送了一些分组数据,最后终端关机。这个数据流示例是现实的,比如一个 WAP 浏览会话。

当终端关机时,它和网络之间没有任何活动。终端开机后执行 IMSI 连线过程,UE 被网络识别。信令连接的建立使 RRC 状态从"空闲"变为"连接的小区(FACH)"状态,FACH 是前向接入信道。同时 PMM 状态从"离线"变为"连接",网络这时有了用户位置的有效信息。SGSN 在"UE 初始消息"中得到这个信息,包括请求活动的信息。当 IMSI 连线成功时,UE 启动"PDP 报文激活"。在这个过程中,UE 和网络协商所期望的分组连接特性,比如 QoS 等级。"PDP 报文激活"的结果是 SM 从未激活状态变为激活状态。

如果需要传输分组数据,就建立一个能携带用户数据流的承载。SGSN 在 UTRAN 上启动 RAB 分配过程,CN 承载在 SGSN 与 GGSN 之间建立。此时网络可同 UE 传输分组数据。RRC 状态用于优化 UTRAN 资源。当 RRC 处于"连接小区 FACH"状态时,只有少量数据可在 Iu 接口传输。在这种 RRC 状态下,UE 和网络之间没有专用连接。如果分组数据量更大一些,就给 UE 分配一个专用信道,RRC 状态则变为"连接小区 DCH",DCH 是专用信道。分组数据传输完毕后,携带用户数据流的 RAB 和 CN 承载被清除,但 PDP 报文继续保留。另外在这个例子中,形成 UE 和网络之间信令连接的信令承载也保留。当数据业务被清除时,RRC 连接状态变为"连接 URA PCH",以节约 UE 的资源。在这种 RRC 状态下,网络不知道 UE 的确切位置,如果网络希望与 UE 通信,就必须寻呼 UE。

如果过一会之后 UE 再次希望向网络发送分组数据,它就向网络发送一个"业务请求"消息,RRC 连接状态再次变为"连接小区 FACH"。"业务请求"触发网络分配 RAB 和 CN 承载。注意这些承载是根据 PDP 报文中的参数分配的。这些承载建立后,UE 就可以收发分组数据。数据传输完成后,携带用户数据流的承载被清除,但 PDP 报文仍保持激活状态,信令连接也继续保留。

对于 UE 被叫的分组数据,GGSN 向服务目标 UE 的 SGSN 发送数据包。SGSN 收到数据包后向目标 UE 发送分组呼叫,分组呼叫强制 UE 把 RRC 状态从"连接 URA PCH"变为"连接小区 FACH",然后 UE 向网络发送"业务请求"消息。因为 SM 处于激活状态,网络就可以根据正确的、经过协商后的连接描述参数来分配 RAB 和 CN 承载。之后,分组数据就传给 UE,如果 UE 也有数据要传就发送给网络。当分组数据发送完成后,携带用户数据流的 RAB 和 CN 承载被清除,只保留信令承载。

用户关机将产生"PDP 报文去激活"过程。此过程将清除网络中储存的与本次分组连接有关的所有地址信息,并删除 PDP 报文,触发 SM 状态从激活变为未激活,从而不能再进行分组数据传输。由于 UE 自行关机,不再需要信令连接,从而被释放。因此,PMM 状态变为"离线",RRC 状态变为"空闲"。

6.3 计费、账单及结算

本节简要介绍UMTS中的计费、账单和结算机制及其用途。先来澄清这些术语的含义。

- 计费是产生计费数据的一些过程。这些过程位于CN单元中。UMTS标准在公共级别上定义了计费(即收集数据的识别)。
- 账单是对计费数据的后处理,其结果就是终端用户的账单。这个过程在UMTS标准之外,由当地法规及其市场情况制约。
- 结算是一个预定时间段内计费数据的总和。结算和计费的区别是:结算收集的信息来自运营商和各个商业体之间的连接,因此结算与终端用户没有直接关系。另外,在电信中,结算和计费是不同的,但在因特网中这两个词经常按同义词使用。

6.3.1 计费和结算

由于历史原因和传承特性,UMTS网络必须能支持针对终端用户业务识别和计费的三种触发,它们是如下三项。

- 基于时间的触发:系统收集关于事务持续时间的信息,包括什么时候开始、什么时候完成、用了多长时间。
- 基于流量的触发:系统收集事务期间所传输的比特数量信息。
- 基于质量的触发:系统收集事务期间有关质量准则的信息。事务的质量配置/准则称为QoS(服务质量)。第8章简要介绍QoS及其参数和机制。

其中第一个传统上用在CS中(如PSTN)。另外两个是几年前因GPRS应用而引入到蜂窝网络中的。由于UMTS能提供很多可能的事务,上述触发可能不够。另外,网络模型的演进更加复杂,且有大量的商业实体涉入。因此,对计费的要求可简列如下。

- 计费应能对同一会话中不同的媒体类型(如语音、视频和数据)和不同的服务(呼叫、流媒体和文件下载等)分别进行。
- 对于同一会话中的媒体或服务,计费应能对不同的QoS等级分别进行。
- 必须能对会话或呼叫的每个臂单独计费。包括呼入和呼出臂,转发和重定向臂。这里所说的臂都是逻辑臂,对实际的信令流和业务流不一定相同。
- 计费可以基于所使用的接入方法(如2G、3G或补充接入方式)。另外,运营商可以选择与接入无关的计费方法,按实际业务使用计费。
- 当用户漫游时,归属网络必须能够按相同的情形进行计费,就像在本地计费一样。例如,若本地计费对流媒体音乐是基于时长的,那么当用户漫游的时候,也必须能做到这一点。
- 必须能让运营商选用GSM/GPRS网络中的计费机制,如基于时长的语音呼叫、基

于流量的数据传输(如流媒体业务、文件下载和浏览)以及按事件(即按次)计费。

- 必须能根据定位、即时通信及推送(push)业务等来进行计费。
- 必须能够使用预付费、后付费、通知付款和第三方付款技术。
- 当用户在归属 PLMN 范围内漫游时,无论被叫用户的归属 PLMN 是否和主叫相同,归属网络必须能够对用户发起的国内呼叫和短信采取不同的资费,而不是只看被叫用户的 MSISDN。

这些要求在商业环境中组合后,其情形如图 6.24 所示。

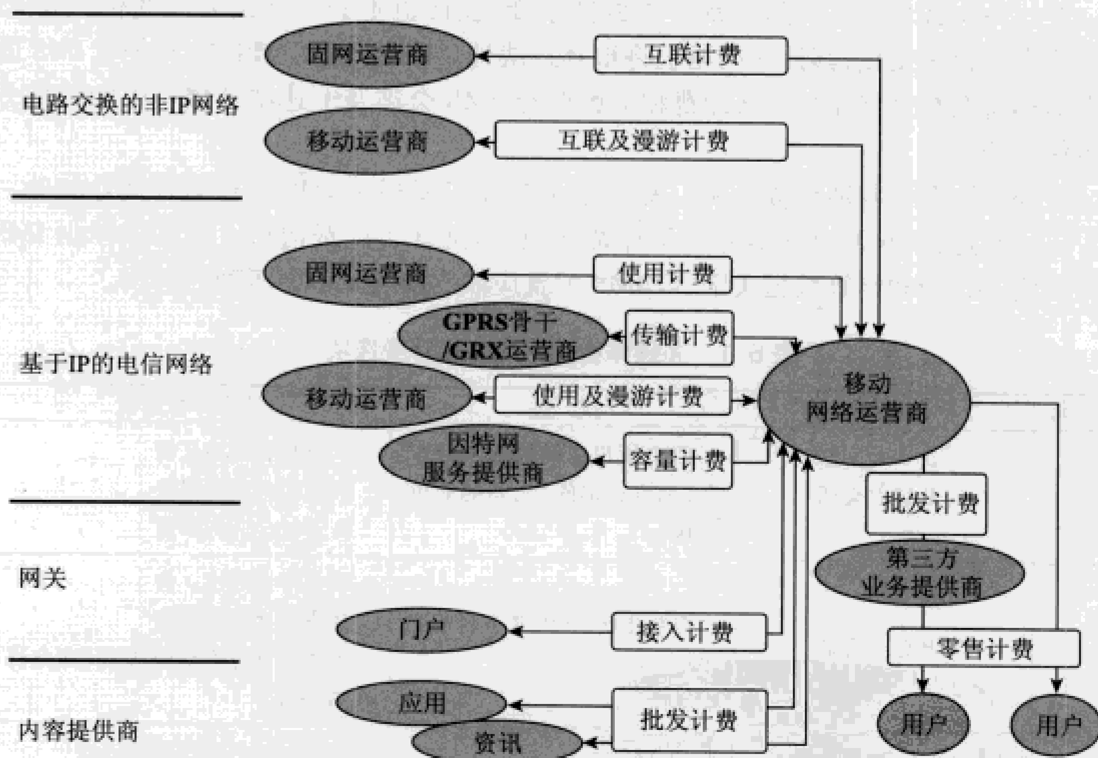


图 6.24　3GPP TS22.115 中定义的计费类型

图 6.24 中有许多商业体。本节主要考虑的是"零售计费"及其要求。零售计费和本节开始所定义的计费是同一意义的。图 6.24 中标出的其他计费方式基本都是结算(终端用户直接看不到)。

一种典型的结算情况是"批发计费",此时虚拟运营商/业务提供商购买网络容量,再卖给它的用户。这种生意现在越来越多。在许多国家,政府对结算接口的价格进行调控以保证竞争。芬兰就是一个很好的例子,当地政府保证各移动网络运营商对各虚拟运营商有公共均等的定价(任何一个虚拟运营商原则上都可以从任何一个移动网络运营商购买网络容量)。

包括"批发计费"在内,移动网络运营商一共有四种结算接口:非 IP 电信网络、基于 IP 的电信网络、各种网关以及服务和内容提供商。非 IP 电信网络主要是 CS,与这

些网络的互连有两种方法。如果CN包含CS域,就直接采用3GPP R99中定义的方法互连。控制平面由SS7和ISUP类型的信令负责,用户平面是PCM中继上的时隙。如果CS域是按照3GPP R4实现的,那么用户平面通过CS-MGW单元互连,相关的信令通过信令网关功能处理。在这两种情况中,结算数据体现了CS资源的利用情况,计费主要基于呼叫时长。对于基于IP的电信网络,结算数据包含了会话信息,包括会话类型和会话中的事务类型。在网关(门户)方面,结算信息包含访问数据(即门户的使用频率)。在内容提供者方面,结算信息反映某一内容的访问次数、访问时间及访问者。

在这一块,CS事务及其计费方式保持不变,预计也不会有什么大的变化。而PS通信将会有很多变化,其计费问题也将很具挑战性。PS通信由IMS进行处理,IMS的体系结构将在6.4节介绍。从计费和结算来看,IMS会涉及上述结算接口中的大部分和零售计费。

表6.1给出了各种计费选项。表中的A、B和C是通过IMS进行多媒体业务的一方。正如所述,表6.1中给出的只是计费选项,不是真实计费情形。最终账单由IMS根据收集的计费和结算数据决定,但IMS配置应能支持表6.1中所列的选项。

表6.1 多媒体会话中的可用计费选项

序号	连接	描述	所需计费选项
1	A与B建立会话	两个用户之间或用户与业务(如语音邮件)之间的简单连接	A支付会话建立费 A支付会话资源费 B支付会话资源费
2	A与B建立会话	简单连接,其中B为名费业务(如800)	B支付会话建立费 B支付会话资源费 A支付部分会话资源费(即允许A、B分账)
3	A请求与B建立会话,B重定向至C	这是重定向。B没有建立与A的连接路径,而是通知A直接与C建立连接	A支付与B的会话建立费 A支付与C的会话资源费 C支付与A的会话资源费 A支付会话资源费如同它与B建立了连接;B支付与C的会话资源费,如同会话来自B
4	A请求与B建立会话,B转发到C	这是和GSM系统中一样的一般中继。连接路径为:A到B的归属网络,B的归属网络到C	A支付与B的会话建立费A支付会话资源费,如同它与B连接,B支付与C的会话资源费
5	A与多方建立会话	与多方的连接都是由A发起	A对每个会话支付建立费 A对每个会话支付资源费 每个被叫方支付与A会话的资源费

（续）

序号	连接	描述	所需计费选项
6	A 有多方会话，会话由每一方与 A 建立	与 A 会话中的每一方是会话的发起者	每一方支付与 A 会话的建立费 A 支付多方会话的资源费 每一单方支付与 A 会话的资源费
7	A 与 B 进行会话，然后 B 保持与 B 的会话，建立与 C 的会话，与 C 结束后又返回 B	A 与 C 会话期间，它与 B 仍然连接。和 C 的会话结束后继续和 B 的会话	A 支付与 B、C 的会话建立费 A 支付会话 B、C 的会话资源费 B 和 C 支付与 A 会话的资源费
8	A 与 B 在会话中，然后应答 C 发出的会话请求，同时保持与 B 的会话	A 与 C 会话期间，它与 B 仍然连接。和 C 的会话结束后继续和 B 的会话	A 支付与 B 会话的建立费 C 支付与 A 会话的建立费 A 支付与 B、C 会话的资源费 B、C 支付与 A 会话的资源费
9	A 与正在另一网络中漫游的 B 建立会话	连接是从 A 到 B 的归属网络，然后中继到位于拜访网络中的 B（正常 GSM 机制） 也可以是，A 被直接重定向到拜访网络中的 B	A 支付与 B 的会话建立费 A 支付会话资源费，如同 B 也在归属网中；B 在其归属网络中支付与拜访网络会话的资源费 A 支付拜访网络中与 B 会话的资源费 B 支付与 A 的会话的资源费

多媒体会话是由媒体成分组成的。根据本节开头给出的要求，网络必须能够识别出各种媒体成分并能相应处理计费和结算数据。

认可的媒体成分有以下几项。

- 语音。
- 实时音频。
- 流音频。
- 实时视频。
- 流视频。
- 数据下载/上传。
- 交互数据（如网页浏览）。
- 消息（SMS 和 MMS 类型）。
- 邮件。
- 不确定内容的数据流，此时网络运营商是一个“比特管道”，计费基于流量（传输的比特数）和质量（所用的 QoS 配置）。

表 6.2 总结了对不同的媒体成分可用的计费机制和类型选项。

表6.2　计费机制和类型选项

成　分	计费机制选项	计费类型选项
语音	计费原则如表6.1所示	按会话时长计费 按请求的和(或)传送的QoS计费 按会话建立计费
实时音频和视频	计费原则如表6.1所示	按会话时长计费 阿布请求的和(或)传送的QoS计费 按会话建立计费
流音频和流视频	对请求发起者计费 对音频和视频的发送者计费	按会话时长计费 按流量计费,可选按QoS差别计费 按会话建立计费
数据(上传和下载)	对请求发起者进行计费 对数据发送者计费	根据会话时长计费 根据流量计费,可选根据QoS差别计费 按会话建立计费
交互数据	对会话请求发起者计费	按时长计费 按流量计费,可选按QoS差别计费 按会话建立计费
消息(SMS、MMS类型)	对消息发起者计费 对消息接收者计费	按事件(如SMS)计费 按流量计费
不确定内容(数据流)	对会话发起者计费 对所有会话方计费	按会话时长计费 按流量(发送及接收)计费,可选按QoS差别计费 按会话建立计费

6.3.2　账单

账单不在UMTS标准范围内,它由UMTS网络之外的设备单独实现。账单的基础是运营商从其网络中收集的计费和结算数据,也有可能包括来自其他网络的数据。

账单处理受当地政府和法律调控,因此各国的处理原则有所不同。除了计费和结算信息外,账单处理还需要其他的源数据,如下所示。

- 用户信息。此信息表明终端用户和运营商/业务提供商之间的业务关系,包括提供的业务、QoS配置和用户身份等。
- SLA(互连/业务等级协议)。它定义了运营商、业务提供商和内容提供商之间的业务关系,包括带宽、QoS保证和运维相关问题等。
- 价格机制。它由运营商/业务提供商制定,并受市场调控,有时也受政府调控,包括每呼叫的价格、每会话的价格、媒体成分的价格、月使用费和降价等。

账单处理的功能就是把这几项同计费和结算数据结合起来,形成最终用户和其他相关方的账单。

6.4 IP 多媒体子系统

本章前几节介绍了 CN 域的结构及 CN 中的管理和控制任务。本节介绍整体结构中的最后一个组成单元,即 IP 多媒体子系统(IMS),它可以使移动设备中的应用建立起对等(peer-to-peer)连接。

人们有分享体验的本性:分享所见、分享所做的事情和分享情感等。现在人们可以用电话交谈,用 MMS(多媒体消息服务)发送图片和语音片段,并可以通过终端浏览网页。或许有人会认为这就足够了,但大量的其他多媒体通信已经涌现,如交互游戏、交互 Web 网服务、应用共享、视频通信、多元化消息、即时通信和集群通信(如 PoC)。同时,许多新业务将会出现。

UMTS 网络通过 GPRS、EDGE 和 WCDMA 给终端带来了灵活的 IP 承载和出色的数据能力。但网络缺少一种机制来连接 IP 终端。这就是 IMS 引入的地方。如图 6.25 所示,IMS 通过在 PS 域使用 SIP 引入了多媒体会话控制,使用户能与各种 AS 建立链接,特别是能在终端之间使用 IP 业务。

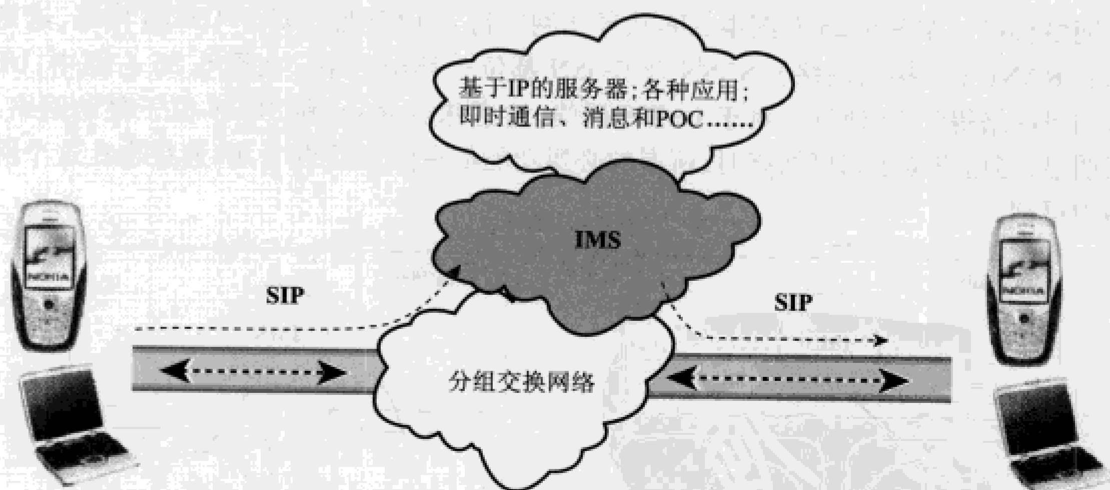


图 6.25 IMS 在分组域中引入了多媒体会话控制

下面介绍 IMS。我们将介绍 IMS 的设计原理,使读者对 IMS 组成模块、不同功能的连接以及 IMS 的关键协议有个初步了解。不过本章主要讲述例子和协议行为。关于 IMS 的详细完整描述,读者可参考 *IMSI IP Multimedia Concept and Service in the Mobile Domain* 一书。

6.5 IP 多媒体子系统基本原理

有一些基本要求指导着 IMS 体系结构的建立及其未来演进。下面 10 项形成了 IMS 结构的基础。

- IP 连接性。
- 与接入无关。
- 分层设计。
- Qos(服务质量)。
- IP 策略控制。
- 安全通信。
- 计费。
- 漫游的可能性。
- 与其他网络互通。
- 对基于 IP 应用的业务开发和业务控制。

“IP 多媒体子系统”这个名称说明,访问这个系统的基本要求是终端必须有 IP 连接性。P2P 应用要求端到端连接,使用地址充裕的 IPv6 最容易实现这一点。因此,3GPP 规定 IMS 只支持 IPv6[3GPP TS 23.221]。不过早期的 IMS 实现和部署使用 IPv4。如果用 IPv4 访问[3GPPP TR 23.981],我们有一个研究报告提出了相关的方针和建议。当用户进行漫游时,IP 连接可从归属网络获得,当用户漫游时,也可以通过拜访网络获得。在图 6.26 左图中,UE 从拜访网络得到 IP 地址。对于 UMTS 网络,这意味着 RAN(无线接入网络)、SGSN 及 GGSN 都位于拜访网络。在图 6.26 右图中,UE 从归属网络得到 IP 地址。对于 UMTS 网络,这意味着 RAN 和 SGSN 位于拜访网络。很明显,当用户位于归属网络时,所有的必要功能都在归属网络中,IP 连接也在这个网络中得到。

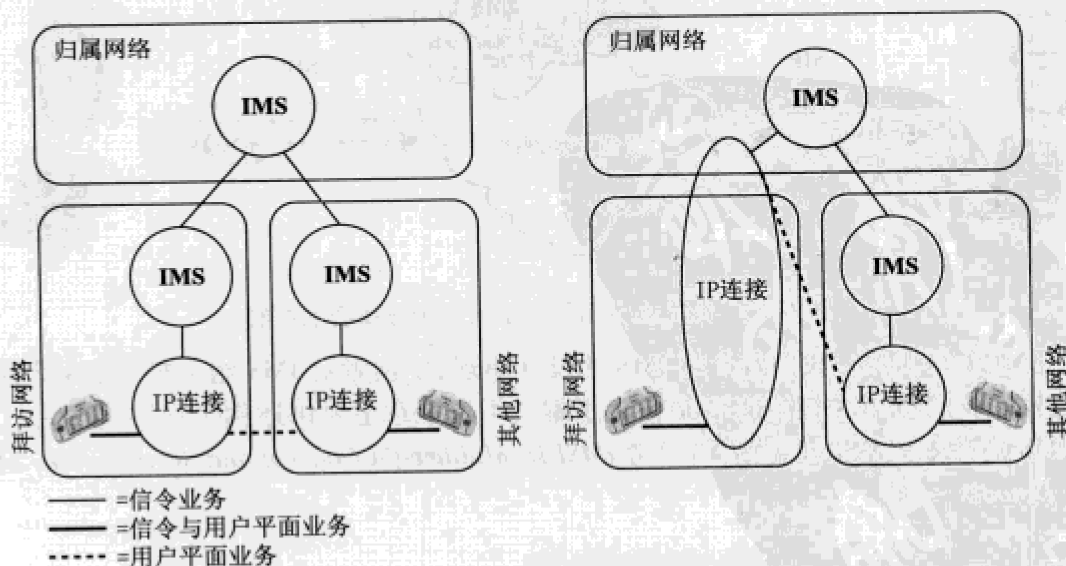


图 6.26　用户在漫游时 IP 多媒体子系统的连接选择

尽管本书针对的是 UMTS 网络,但必须认识到,IMS 被设计得与接入无关,因此 IMS 业务可以在任何有 IP 连接的网络上提供,如 GPRS、WLAN 和宽带接入 xDSL。实

际上,IMS 的第一版(R5)是和 UMTS 绑定的,因为唯一可能的 IP 连接接入网就是 GPRS。但第二版(R6)中标准已经进行了修正,使所有其他接入方式都成为可能。

除了与接入无关外,IMS 体系结构是基于分层的。这就意味着传输和承载业务是和 IMS 信令网及会话管理业务分开的。更高层次的服务在 IMS 信令网的顶层(见图 6.27)。分层的目的是为了尽量减少各层之间的依赖性。它的好处之一就是便于增加新的接入网。3GPP R6 中的 WLAN(无线局域网)接入 IMS 将对此做出验证。其他接入方式(如固网宽带)将可能随后跟进。这种分层的方式提升了应用层的重要性。由于应用是单独的层,并用 IMS 网络能提供各种公共功能,因此相同的应用可以运行在使用不同接入方式的 UE 上。

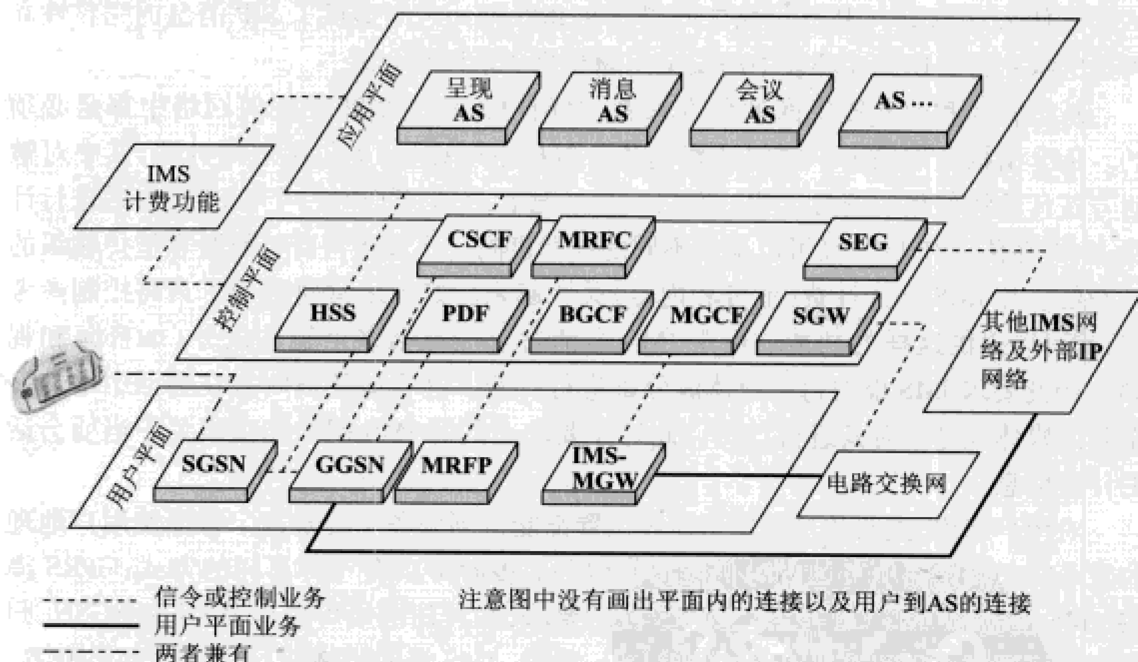


图 6.27 IMS 及其分层结构

QoS 在 IP 网络中扮演着非常重要的角色,因为,众所周知,延迟长且易变,分组会无序到达,有些分组会在因特网上完全丢失。IMS 端必须要改变这一点,否则终端用户就不会去用最新的 IMS 服务。在 IMS 中,UE 在 SIP 会话建立或修改时协商其能力并申明其 QoS 要求。可协商的参数包括:媒体类型、业务方向、媒体比特速率、分组大小和分组传输频率。完成应用级的参数协商之后,UE 便能把信息映射到 UMTS QoS 参数,并能在 RAN 和 GPRS 网络中预留适当的资源。第 8 章讲述 QoS 的分类、属性以及相关的网络机制。我们已经介绍了,为了实现端到端的 QoS,UE 是怎样保证 UE 和 GGSN 之间的 QoS 的。此外,还需要在 GGSN 之间进行连接来提供必要的 QoS。这一点可以通过运营商之间的 SLA 来完成。

IP 策略控制是对 IMS 媒体使用承载业务的鉴权和控制能力,其基础是 IMS 会话

的信令参数。它要求GPRS网络和IMS之间能够交互。

- 当激活媒体业务承载时，策略控制单元能核实SIP信令所协商的值是否被采用。运营商因而能确信其承载资源以SIP信令的协商值用于特定的P2P连接（在SIP信令中协商的）。
- 策略控制单元控制SIP会话端点之间的媒体业务何时开始或停止。
- 策略控制单元可以从GPRS网络接收关于用户PDP报文的修改、停止或去激活通知。

安全是UMTS网络每一部分的基本要求，IMS也不例外。除了GPRS网络中的认证鉴权过程之外，IMS在UE和IMS网络之间有其自己的认证鉴权机制。此外，不论接入网是什么，在UE与IMS网络之间以及在IMS网元之间提供了SIP消息的完整性和可选的机密性。UMTS环境中的安全问题在第9章详细介绍。

从运营商和业务提供商的角度来看，对用户计费的功能在任何网络中都是必须的。IMS结构允许采用不同的计费模式。包括主叫计费，也包括双向计费，其中对被叫方按传输级使用的资源计费。在后一种情况下，完全可以对一个IMS级会话进行计费，也即在传输和IMS级可以采用不同的计费机制。不过运营商可能愿意把传输级的计费信息和IMS级的计费（业务和内容）关联起来。如果运营商利用了策略控制参考点，就可以提供这样的功能。由于IMS会话有可能包括多个媒体成分（如音频和视频），因此要求IMS能对每一媒体成分都进行计费。这将能使被叫方在会话中增加一个新的媒体成分时对其进行计费。此外还要求不同的IMS网络能交换关于当前会话的计费信息。

对用户来说，重要的是在任何地理位置都能得到服务。漫游这个特征使用户地理位置不在归属网络服务区内时仍能得到服务。漫游可以有三种不同的方式：GPRS漫游、IMS漫游和IMS CS漫游。GPRS漫游要求，在拜访网络可提供RAN和SGSN、归属网络可提供GGSN和IMS时，能够接入IMS。IMS漫游模式指这样一种网络配置，其中拜访网络提供RAN、SGSN、GGSN和IMS入口（即P-CSCF），归属网络提供其余的IMS功能。IMSCS漫游指IMS域和CS CN域之间的漫游。就是说，如果IMS不能到达用户，就把会话路由至CS CN，反之亦然。

可以预见，不同类型的网络在未来许多年之内将继续共存。因此与现有网络（PSTN、ISDN、移动网和因特网）之间的互通对任何新的网络结构来说都是一个重要的方面。此外，有些用户可能不乐意更换其终端或改变他们定制的业务来适应新的技术革新，还有一些用户可能使用多个不同能力的终端：如在办公室中使用WLAN（无线局域网）终端，在户外使用UMTS终端，在家中使用有线终端。由此产生的问题就是必须达到用户，不论他在哪里和他使用的终端是什么。作为一个新的成功网络技术和结构，IMS应该能够连接更多的用户，因此IMS支持与PSTN、ISDN及移动和因特网用户的通信。

CS CN和IMS在业务控制模型和业务部署方面不同。CS CN采用访问业务控制

就是说，当用户进行漫游时，由访问网络中的一个实体为用户提供服务和控制，该实体称为 VMSC(拜访移动交换中心)。与此相反，IMS 采用归属业务控制，控制业务的 S-CSCF(服务会话控制功能)总是位于归属网络中。可扩展性业务平台和迅速开通新业务的重要性意味着不再用那种老式的方法来完全标准化各种电信业务、应用和补充业务。由于这个原因，IMS 提供了一个业务框架，该业务框架可以提供必要的能力来支持各种多媒体应用。实际上，IMS 本身并不是一种业务，而是一种基于 SIP 的体系结构，用来在 PS 网络之上实现高级的 IP 业务和应用。IMS 为实现业务提供了必要的手段。这一类应用有比如即时通信和会议通信。未来的预期是，OMA(开放移动联盟)将开发出各种各样的应用和服务，最大程度地利用 IMS。

6.6 IMS 实体及功能

本节讨论 IMS 实体和关键的功能。这些实体可以大致分为以下六类。

- 会话管理和路由类(CSCF)。
- 数据库(HSS 和 SLF)。
- 互通功能(BGCF、MGCF、IMS-MGW 和 SGW)。
- 服务(AS、MRFC 和 MRFP)。
- 支持功能(THIG、SEG 和 PDF)。
- 计费。

重要的一点是，IMS 标准并未规定网络实体内部功能的细节，而是规定了实体之间的参考点以及参考点处的支持功能，例如 CSCF 怎样从数据库中得到用户数据。

6.6.1 呼叫会话控制功能

CSCF(呼叫会话控制功能)一共有三类：P-CSCF(代理 CSCF)、S-CSCF(服务 CSCF)和 I-CSCF(查询 CSCF)。每一个 CSCF 都有其特殊的任务。这些 CSCF 在注册和会话建立过程中起作用，并形成了 SIP 路由机制。并且它们都能把计费数据发送给离线计费功能。P-CSCF 和 S-CSCF 有一些共同的功能。它们都能代表用户释放会话(例如 S-CSCF 检测到会话挂断，P-CSCF 接收到媒体承载丢失的通知)，也能够检查 SPD(会话描述协议)净荷的内容，检查是否包含了不允许用户使用的媒体类型和编解码器。如果提议的 SDP 与运营商的策略不匹配，CSCF 就会拒绝请求并向 UE 发送 SIP 错误信息。

6.6.1.1 P-CSCF

在 IMS 中，P-CSCF 是用户的第一个联系点。所有来自 UE 的 SIP 信令都被发送到 P-CSCF。类似地，所有来自网络的 SIP 信令也都从 P-CSCF 发到 UE。P-CSCF 有 4 个不同的任务：SIP 压缩、IPSec(IP 安全)关联、与 PDF(策略判决功能)的交互和紧急呼叫检测。

SIP 是基于文本的信令协议，包含了大量的信头和信头参数，包括扩展信息以及和安全相关的信息，因此 SIP 消息要比二进制编码的协议大。在 IMS 体系中，建立 SIP 会话是一个繁锁的过程，包括编解码和扩展协定，还包括 QoS 互通说明。总体上提供了一个灵活的框架，不同要求的会话都可以建立。缺点是无线接口上交互的数据量大。这一点意味着以下两点。

- 与小区信令相比，使用 SIP 建立会话的时间较长，终端用户在建立会话时将感觉到一个延迟，这是不期望的，也可能是不可接受的。
- 小区内的会话以某一方式严重影响语音质量及系统性能。

为了加速会话的建立，3GPP 要求支持 SIP 压缩。UE 有多种方法可以向 P-CSCF 指示出它期望在空中接口接收压缩的信令消息。

P-CSCF 负责维护 SA（安全关联）以及 SIP 信令的完整性保护和机密性保护。在 SIP 注册时，UE 和 P-CSCF 通过协商 IPSec 实现这一点（第 9 章将对 IPSec 进行详细介绍）。

当运营商采用 IP 策略控制时，P-CSCF 负责把会话及媒体相关的信息中继到 PDF。PDF 根据这个信息导出认可的 IP QoS 信息，GGSN 在接收次要 PDP 报文激活之前根据该信息执行 IP 策略控制。此外，通过 PDF 和 IMS 可以把 IMS 计费相关信息发送到 GPRS 网络，也能接收来自 GPRS 的计费相关信息。这样在账单系统中就可以合并来自 IMS 和 GPRS 的计费数据记录。

IMS 紧急会话尚未完全定义。因此暂时的要求是：IMS 网络检测紧急会话的意图，引导 UMTS UE 使用 CS 网络进行紧急会话。其中的检测是 P-CSCF 的任务。IMS 支持紧急会话后这个功能也不会消失，因为某些漫游情况下，UE 可能并不知道它已经拨打了一个紧急号码。

6.6.1.2　I-CSCF

I-CSCF 是网络运营商和该网络面向的用户之间的联系点。I-CSCF 有如下四个独立的任务。

- 从 HSS 中获得 S-CSCF 名。
- 根据 HSS 中的信息指派一个 S-CSCF。当用户在网络中注册或者未注册的用户接收到一个 SIP 请求而它又想接收与未注册状态相关的服务时，就进行 S-CSCF 分配。
- 路由达到将进一步请求分配 S-CSCF。
- 提供 THIG（拓扑隐藏互通网关）功能（THIG 将在 6.6.5 节进一步介绍）。

6.6.1.3　S-CSCF

S-CSCF 是 IMS 的核心所在，负责处理注册过程、生成路由方案、维护会话状态并存储业务配置。

当用户发送一个注册请求时，该请求会被转到 S-CSCF，S-CSCF 从 HSS 处下载鉴权数据。S-CSCF 根据鉴权数据对 UE 发出认证要求。在收到 UE 的回复并核实通过

后,S-CSCF 就接受注册请求并开始监管注册状态。此后用户便可以初始化并开始 IMS 服务。此外,S-CSCF 从 HSS 下载业务配置也是注册过程的一部分。

业务配置是永久储存在 HSS 中的一些用户信息。当某个特定的公共用户标识(如 vjoe. doe@ ims. exmple. com)向 IMS 注册时,S-CSCF 就下载与该公共用户标识关联的业务配置。S-CSCF 使用包含在业务配置中的信息,当用户发送 SIP 请求或从某处接收 SIP 请求时,业务配置中的信息指示何时,特别是与什么 AS 进行联系。此外,业务配置还可能包括有关 S-CSCF 应用媒体策略类型的进一步说明。例如,它可以指示某个用户只允许使用音频和应用媒体成分,不允许使用视频成分。

对于所有源自或到达 UE 的会话和事务,S-CSCF 负责做出关键路由决定。当 S-CSCF 收到 UE 经过 P-CSCF 发出的请求时,它需要决定是否在进一步发送请求之前联系 AS。在进行了可能的 AS 交互之后。S-CSCF 要么在 IMS 中继续会话,要么中断到其他的域中(如 CS 域或其他 IP 网络)。此外,如果 UE 使用 MSISDN 号来对被叫方进行寻址,那么 S-CSCF 在进一步发送请求之前先把 MSISDN 号(即 tel URL)转化为 IP URI 格式,因为 IMS 不是按 MSISDN 号进行路由的。类似地,S-CSCF 接收所有到达 UE 的请求。尽管 S-CSCF 能从注册中知道 UE 的 IP 地址,但它还是通过 P-CSCF 为所有的请求进行路由,因为 P-CSCF 负责 SIP 压缩和安全功能。在发送请求到 P-CSCF 之前,S-CSCF 也可能会把请求路由到 AS(例如为了检查可能的重定向指令)。图 6.28 显示出了路由决定中的 S-CSCF 的作用。

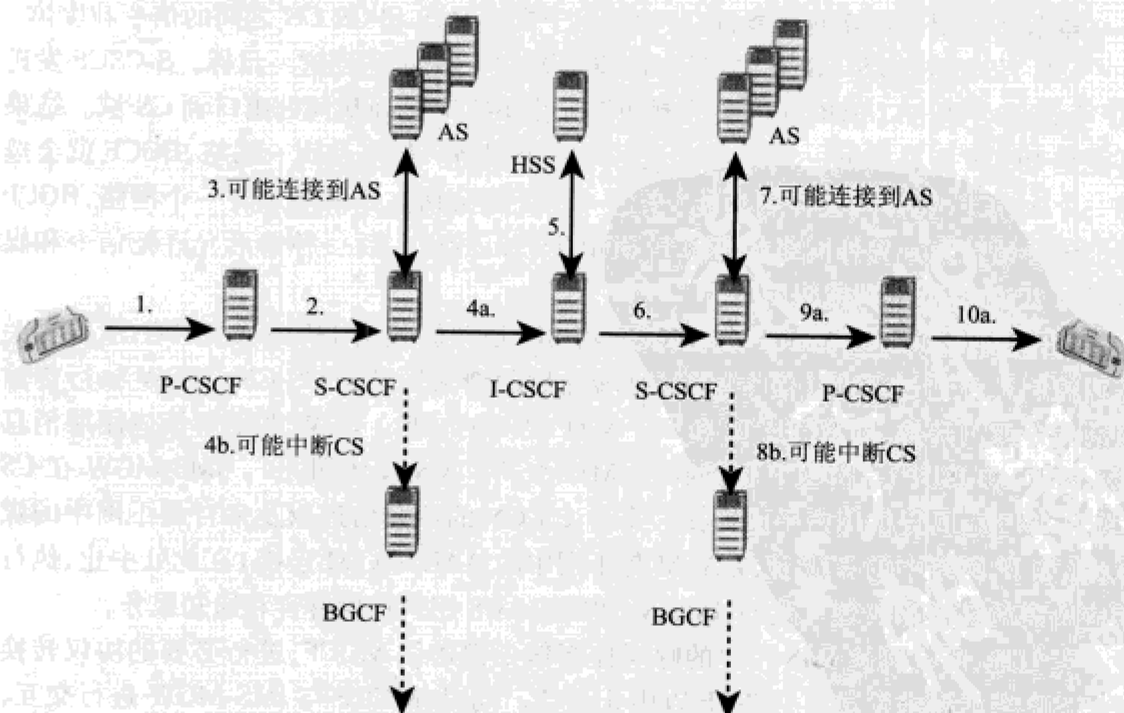


图 6.28 S-CSCF 路由以及基本的 IMS 会话建立

6.6.2 数据库

IMS 体系结构中有两个主要的数据库:HSS(归属用户服务器)和 SLF(签约位置功能)。

HSS 主要存储所有 IMS 的用户和服务相关的数据。存储在 HSS 中的主要数据有用户标识码、注册信息、接入参数和服务触发信息[3GPP TS 23.002]。用户标识码有两种类型,即私有用户标识和公用用户标识(见 6.2.1.1.7 节和 6.2.1.1.8 节)。私有用户标识由归属网络运营商分配,用于注册和鉴权。而公共用户标识使得其他用户可以请求与终端用户进行通信。IMS 接入参数用来建立会话,包括用户鉴权、漫游认证和所分配的 CSCF 域名等参数。服务触发信息用以启动 SIP 业务的执行。HSS 也提供用户特定的要求,该信息用于 I-CSCF 以选择最合适的 S-CSCF。除了和 IMS 相关的功能以外,HSS 还包括 PS 域和 CS 域所需要的 HLR/AuC 功能子集。不同 HSS 之间的通信并没有标准化。归属网络可能有多个 HSS,取决于移动用户的数量、设备的容量和网络的组织结构。

当网络运营商部署了多个不同地址的 HSS 时,SLF 用于使 I-CSCF、S-CSCF 和 AS 能得到给定用户对应的 HSS 地址。

6.6.3 互通功能

本节将介绍四种互通功能,这些功能用于交换 IMS 和 CS CN 之间的信令和媒体。

6.6.1.3 节指出 S-CSCF 决定何时中断 CS CN。为了达到这一目标。S-CSCF 发送 SIP 会话请求到出口 BGCF(网关控制功能),由 BGCF 选择从何处出口到 CS 域。结果可能是 BGCF 所在的同一网络或者是另外一个网络。如果是同一网络,BGCF 就会选择一个 MGCF(媒体网关控制功能)来进一步处理会话。如果是另外一个网络,BGCF 就把该会话转发到另外网络的 BGCF[3GP TS 23.228]。后一种情形允许把信令和媒体通过 IP 就近路由到被叫用户。

SIP 会话请求到达 MGCF 后,MGCF 将 SIP 协议转换为 ISUP(或 BICC,承载无关呼叫控制),再通过 SGW(信令网关)把转化后的请求发送到 CS CN。SGW 执行传输级的信令双向转换,即 SCTP/IP 和 SS7 MTP 之间的转换。SGW 并不解读应用层消息(如 BICC 和 ISUP)。MGCF 也控制着 IMS-MGW(IMS 媒体网关)。IMS-MGW 在 CS CN 和 IMS 之间提供用户平面链接。来自 CS CN 的承载信道以及来自骨干网中的媒体流(如 IP 网络中的 RTP 流或 ATM 骨干网中的 AAL2/ATM 连接)在此处中止,执行相应所需的转换和处理。此外,IMS-MGW 能向 CS 用户提供铃音和通知服务。

类似地,所有到达 IMS 用户的呼叫控制信令都送往 MGCF,进行必要的协议转换并把 SIP 会话请求发送到 I-CSCF 以中止会话。同时,MGCF 与 IMS-MGW 进行交互,为用户平面保留必要的 IMS-MGW 资源。

图 6.29 画出了互通的概念,图中左图是 IMS 发起的会话,右图是 CS 发起的呼叫。

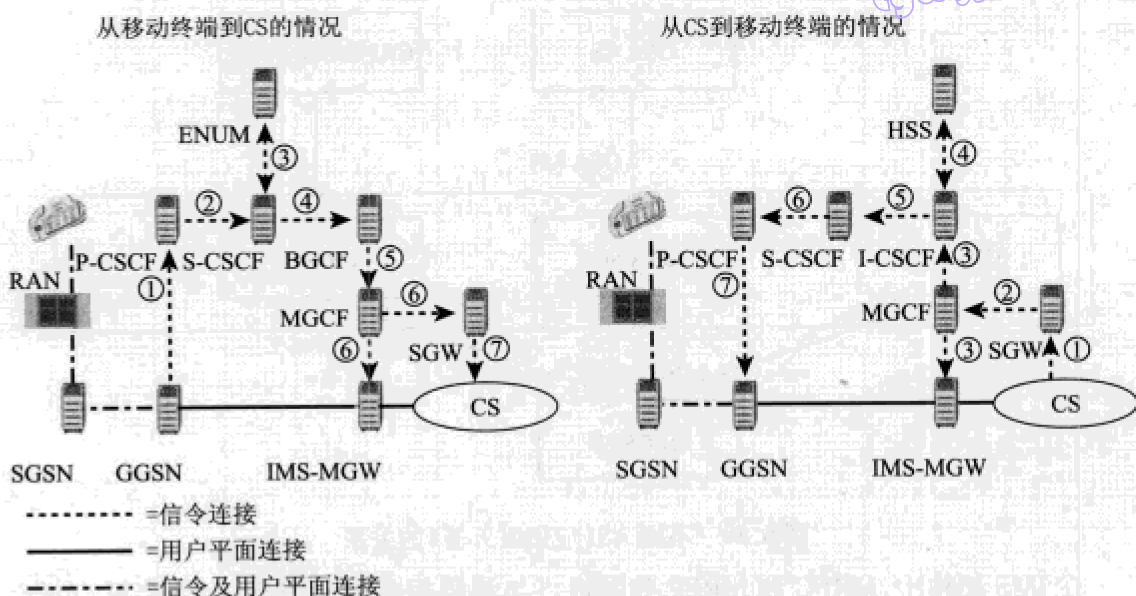


图 6.29 IMS 与 CS 的互通

6.6.4 业务相关的功能

本书把 IMS 业务相关功能分为三类：MRFC（多媒体资源功能控制器）、MRFP（多媒体资源功能处理器）和 AS。

考虑到分层设计思想，AS 并不是纯粹的 IMS 实体，它是 IMS 之上的功能。这里把 AS 放到 IMS 功能中是因为 AS 这个实体可以在 IMS 中提供增值服务，如即时通信和 PoC 业务。AS 位于归属网络中，或者这位于第三方网络或者是一个独立的 AS。AS 的主要功能如下。

- 对来自 IMS 的 SIP 会话进行处理并可能产生影响。
- 可以发出 SIP 请求。
- 可以向计费功能发送结算信息。

运营商也可以通过 CSE（CAMEL 业务环境）和开放业务架构提供业务，因此所提供的业务不限于基于 SIP 的业务[3GPP TS 23.228]。因此，“AS”一词一般指 SIP AS、SCS（OSA 业务能力服务器）和 CAMEL IMS-SF（IMS 交换功能）。

图 6.30 示出了不同功能的连接关系。从 S-CSCF 看来，SIP AS、OSA 业务能力服务器和 IMS-SF 表现为相同的参考点。一个 AS 可能只用于一业务，而用户可能有多个业务，因此对每个用户来说，可能有一个或多个 AS。此外，一个会话也可能涉及多个 AS，例如一个 AS 根据用户的偏好控制业务的终止点（如在 5p.m 到 7a.m 之间把所有呼入的多媒体会话重定向到应答机中），另一个 AS 根据 UE 的能力（如屏幕大小和颜色种类等）调整即时消息的内容。

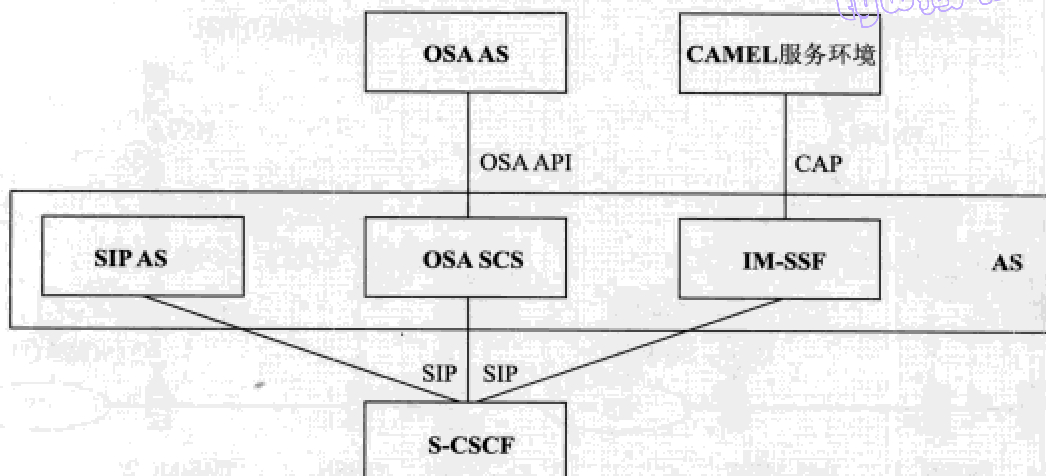


图6.30 不同AS(应用服务器)的关系

在IMS架构中,MRFC和MRFP共同提供与承载相关的业务机制,如会议、布告、代码转换等。MRFC负责处理与S-CSCF的双向SIP通信并控制MRFP。MRFP提供MRFC要求的用户平面资源。MRFP执行下述功能。

- 合并到达的媒体流(如对于多方通信)。
- 媒体流的源(多媒体布告)。
- 媒体流处理(如音频代码转换和媒体分析)[3GPP TS23.228,TS 23.002]。

目前,MRFC和MRFP在IMS架构中作用比较小,因为在IMS会议工作[3GPP TS 24.140],MRFC的位置与AS是在一起的,并且MRFC和MRFP之间的参考点也没完整地定义。

6.6.5 支持功能

把控制平面和用户平面分开可能是IMS设计中最重要的一点。各层之间完全独立并不可行,如果用户平面和控制平面之间没有交互的话,运营商就无法控制QoS、IMS媒体业务的源和宿以及媒体开始和结束的时间。因此需要创建一种机制对IMS媒体业务使用的承载业务进行认证和控制,这一点基于IMS会话中协商的SDP参数。GPRS与IMS之间的总体的交互称作"基于业务的本地策略"(SBLP)。后来又增加了交换计费相关信息的能力。PDF根据来自P-CSCF的会话和媒体相关信息进行决策,它是SBLP控制的决策点。

IMS中的会话建立包括端到端的SIP和SDP消息交换。UE在消息交换中协商一组媒体特性(如公共的解码器)。如果运营商采用了SBLP,P-CSCF将会把相关的SDP信息及其发起者信息中继到PDF。PDF相应分配和返回一个令牌,由P-CSCF传递到UE。PDF把SDP参数映射到认可的IP QoS参数以通过Go接口传输到GGSN,从而PDF可记录并认证已选媒体成分的IP流。如果UE激活或修改了媒体的PDP报文,它必须自行将SDP参数和应用需求映射到UMTS QoS参数。PDP报文激活和修改也包

括所收到的鉴权令牌和流识别码作为绑定信息。接收到 PDP 报文激活或修改信息后，GGSN 从 PDF 请求鉴权信息。PDF 比较接收到的绑定信息和存储的认证信息，返回认证结论。如果绑定的信息有效，PDF 向 GGSN 发送媒体认证的细节信息，包含 IP QoS 参数以及与 PDP 报文相关的分组类别信息。GGSN 把认可的 IP QoS 参数映射到认可的 UMTS QoS 参数，再把这个 UMTS QoS 参数和认可的 PDP 报文中的 UMTS QoS 参数进行比较。如果 PDP 报文请求的 UMTS QoS 参数在 PDF 的限制之内，就接受 PDP 报文的激活或修改。

除了承载认证外，PDF 还接收这样一些信息，包括何时发布 SBLP 主导的 PDP 报文，UE 是否已经丢失/恢复了无线承载，何时 SBLP 主导的 PDP 使用流业务或对话业务等。PDF 根据这些信息向 P-CSCF 通知所发生的事件。这样就能使 P-CSCF 影响计费，并能为用户启动 IMS 会话。此外，PDP 能够请求 GGSN 去激活某个特定的 SBLP 主导的 PDP 报文。

SEG（安全网关）的作用是在安全域保护控制平面业务。安全域是指单一管理机构管理的网络，一般与运营商的边界吻合。SEG 位于安全域的边界处，它强制施行该安全域的安全策略，这些策略指向目的地安全域的 SEG。在 IMS 中，所有业务都经过 SEG 路由，尤其是域间的业务（即发起和接收处在不同的安全域中）。在保护域间 IMS 业务时，保密性、数据完整性和鉴权都是必须的。

THIG 功能可以把网络的配置、容量和拓扑隐藏在运营商的网络之外。如欲使用隐藏功能，那么当从其他 IMS 网络收到请求或响应时，就需要在路由路径中设置 THIG 功能。向其他 IMS 发出请求或响应，也必须在路由路径当中设置 THIG。THIG 对包含 IMS 网络拓扑的头（header）进行加密和解密。

6.6.6 计费功能

IMS 体系结构既可以支持在线计费，也可以支持离线计费。在线计费过程中，IMS 实体（如 AS）与在线计费系统交互工作。在线计费系统又与用户账号实时交互，并控制监视与业务使用相关的计费。例如，AS 在允许会话建立之前先查询在线计费系统或接收关于用户此次呼叫持续时间的信息。离线计费中，计费信息主要是在会话之后收集的，计费系统不会对使用的业务产生实时的影响。在这种模式下，用户一般是按月收到账单，账单出示一定时间段内的计费细节。不同的计费模式需要不同的体系结构。

离线计费体系中的核心是 CCF（计费采集功能）。CCF 接收来自 IMS 实体（P-CSCF、S-CSCF、I-CSCF、BGCF、MGCF、AS 和 MRFC）的结算信息。进一步处理后建立格式化的 CDR（计费数据记录）。CDR 传到账单系统，它综合考虑了其他来源（如 CGF）的结算信息后形成最终的 CDR，然后生成实际的账单。账单应包括会话数量、被叫方、会话持续时间和会话类型（如音频、文本和视频）。

能进行在线计费的 IMS 实体是 S-CSCF、AS 和 MRFC。当 UE 向需要鉴权的 AS、MRFC 或 S-CSCF 提出某种请求时，这些实体先联系 OCS（在线计费系统），再向用户

传送业务,例如用户可以发送一个请求到新闻服务器定制最新的赔率,或者定制一个语音会议。OCS 支持两种不同的鉴权模式:立即事件计费和单元保留事件计费。立即事件计费模式用 OCS 的费率功能得到该事件的资费标准。有了费率和价格后,就在用户账号上生成具体的费用,然后 OCS 对来自相关实体的请求(AS、MRFC 和 S-CSCF)进行授权。使用该模式时,IMS 实体应能确定它可以把请求业务发送到用户。例如 AS 发出一个请求,并向 OCS 通知业务类型(如象棋游戏)和数量(比如说 2)。然后 OCS 使用费率功能确定出资费(比如说 0.3 欧元),再根据数量计算出价格(0.6 欧元),最后在用户账单上生成费用 0.6 欧元,然后 OCS 通知 AS 授权 2 个单元。在单元保留事件计费模式中,如果请求中没有给出费用,OCS 用费率功能并根据具体业务信息来决定所期望服务的价格。然后 OCS 在用户账户上保留一定数量的费用,再向请求实体(AS、MRFC 或 S-CSCF)返回相应的资源数量。资源的数量可以是时间或者流量。如果授权给用户的资源已经被用光,或者业务已经完成或终止,IMS 实体将会告知 OCS 用户已经消费的资源数量。最后,OCS 从用户账户上生成一个费用[3GPP TS32.200,TS32.225,TS32.2601],但可能需要进一步与费率功能交互。这种模式适合于 IMS 实体(AS、MRFC 或 S-CSCF)不能事先确定能否发送业务,或者不能事先确定所需资源(如通话时间)的情形。

第 7 章 UMTS 终端

就终端用户来说，UMTS 终端是 UMTS 系统最明显的网络功能单元。因此，经常把它视为向终端用户提供应用接口和服务的单元。然而这只是很小的一部分，终端的实际功能要更为宽泛一些。本章旨在简要介绍 UMTS 终端的结构及其结构外的功能，以便了解其能力和制约。

需要注意的是，从网络来看，终端的总体协议结构和功能都必须符合标准的规定。尽管如此，它们的实现和其他内部功能却完全取决于具体实现，这一点也正是移动通信市场中的一个重要竞争因素。因此，本章对终端结构的描述主要基于相应的规范进行，这正是接近该有趣主题的一个方法。

7.1 终端结构

在 UMTS 中，无线接口的移动用户终端设备的学名是 UE（User Equipment，用户设备），通常简称为"终端"。从网络的观点看，UE 负责在无线接口另一端需要的通信功能，这些功能不包括终端用户应用。UMTS 终端的必备功能模块主要与终端和网络之间的交互作用相关。以下功能是所有 UMTS 终端必备的。

- 提供在集成电路卡上插入 UICC（Universal Integrated Circuit Card，通用集成电路卡）的接口，该卡包含 USIM（Universal Subscriber Identity Module，通用用户识别模块），可选的 ISIM（INS Identity Module，IMS 识别模块应用）。
- 提供业务与注册和注销网络。
- 更新位置。
- 发起或接收面向连接或无连接的业务。
- 不可变更的 IMEI（设备识别码）。
- 基本的终端识别能力。
- 在没有 USIM 的情况下，终端必须能够支持紧急呼叫。
- 支持认证和加密算法的执行。
- 除了这些网络操作的必备功能外，为了今后的演进，UMTS 终端还应支持以下功能。

○ API(Application Programming Interface,应用程序接口)功能。

○ 能把业务相关信息(参数、脚本或软件)、新的协议、其他功能乃至新的 API 下载到终端的机制。

○ 可选择插入多种 UICC 卡。

展现在人们面前的 UE 通常是一个单独的集成设备,因为厂商销售的就是这个物理上不可分割的设备。但在成熟的移动系统中,UE 至少从标准上说通常是一些互连的模块,各个模块有独立的功能群。这些模块有时也作为分立的部件在物理上实现,但不管怎样,这些功能群或子群在网络一端都有对应的部件。

例如 GSM 系统的主要创新之一就是通过定义标准接口,从物理上把与用户相关的 SIM(Subscriber Identity Module,用户识别模块)和与通用电信系统相关的部分分开。UMTS 也继承了这一思想,它使用户、运营商以及物理终端互相独立。

另一个重要的分离是无线接入网络与跟核心网相关的部分之间的分离。但是它不是标准的内容,相反它由提供商在实现终端时根据实际安排进行考虑。这一模块使终端至少在内部能制造为多模/多网络终端,也便于无线接入技术从核心网中独立出来。图 7.1 显示出了此处所讨论的用户设备的参考结构,以及网络侧相关的对应部分。

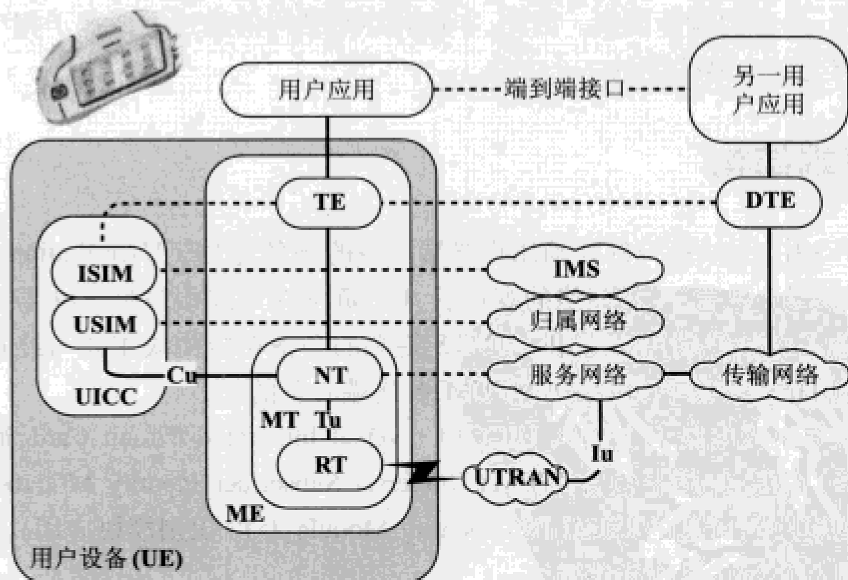


图 7.1 UE 的参考结构

UE 由 ME(mobile equipment,移动设备)和 UICC 组成。

UICC 是 ME 中与用户相关的部分。它包含一个或多个 USIM 以及相应的应用软件。USIM 本质上是一个逻辑概念,在 UICC 中物理实现。UICC 也可以针对 IMS 服务包括可选的 ISIM 应用。由用户所属的运营商以任何方式提供 USIM 信息内容。USIM 涉及的是业务方面,而不是用户方面。ISIM 只是为了用户和网络鉴权以及重要 IMS 业务约定。

ME 是 UE 中与用户无关的部分，由不同的模块构成。

ME 中的 TE(Terminal Equipment，终端设备)部分是向终端用户提供应用功能的设备，如呼叫控制客户端、IP 和其他的数据终端、IMS 媒体编码和会话管理客户端。TE 知道代表用户应用的可能的标准电信业务，它也是电信业务平台的终点。

从另一方面讲，MT(Mobile Termination，移动终端)是 ME 中这样一个部分，它是网络进行无线传输的终结点，并能根据无线传输的要求调整 TE 的容量。从移动系统的角度看，MT 基本就是实际的终端设备，它能改变在接入网络中的位置，并能移动到采用相同接入技术的其他接入网络的覆盖区域中。MT 也是 UMTS 网络系统的业务终结点。

MT 的 NT(Network Termaination，无线终端)功能群是 MT 中与核心网相关的部分。NT 采用非接入层协议来进行 MM/GMM(移动性管理/GPRS 移动管理)和 CM/SM(通信管理/会话管理)。所以，从纯粹的核心网角度看，NT 可以视为终端。非接入层协议在第 10 章介绍。

MT 的 RT(Radio Termination，无线终端)功能群只和无线接入网络相关。它包含对所有业务都相同的功能，这些业务采用同一特定的 RT 无线接入技术。RT 在物理无线连接之上采用接入层协议，如 MAC(Media Access Control，媒体接入控制)、RLC(Radio Link Control，无线链路控制)和 RRC(Radio Resource Control，无线资源控制)。所以从 UTRAN 的角度来看，RT 可视为终端。MAC、RLC 和 RRC 协议也在第 10 章介绍。

本书按上述的功能群来描述终端结构。表 7.1 是它们与网络侧的业务和子系统的关系的总结。图 7.2 所示的主要功能实体和以上功能群中的对应关系清楚地表明了它们的实质。

表 7.1　UE 功能群总结

	关　系	在终端侧的终结点	在网络侧的对应部分
UE	在电信设施中与用户应用或者用户接口无关的部分	终止用户间和应用无关的电信系统	对应传输网络后的固定或者移动用户设备
UICC	UE 中与用户和用户定制相关的部分	最后终止所有与用户相关的安全和业务控制活动	电信业务提供商的定制管理系统
USIM	UICC 中与用户的 UMTS 定制相关的部分	主要是在归属网络中终止与用户相关的控制功能	一般来说，归属运营商管理用户的归属网络寄存器(例如 HLR 和 HSS)
ISIM	UICC 中与用户的 IMS 定制相关的部分	在 IMS 中终止与用户相关的控制功能	由运营商管理的用户 IMS
ME	UE 中与用户定制无关、与移动系统相关的部分	终止所有控制平面功能以及用户平面的 UMTS 承载	整体 UMTS 网络
TE	ME 中与电信业务平台相关，与移动系统基本无关的部分	终止由 UMTS 承载所传输的通信业务	在外网后的对等终端设备

（续）

	关　系	在终端侧的终结点	在网络侧的对应部分
MT	ME中与UMTS相关，与电信业务基本无关的部分	终止UMTS网络系统业务	由主动接入的运营商（拜访运营商）管理的UMTS系统
NT	MT中与核心网相关、与无线接入网络无关的部分	终止UMTS核心网业务	UMTS CN
RT	MT中与无线接入技术相关、与核心网无关的部分	终止UTRAN业务	UTRAN

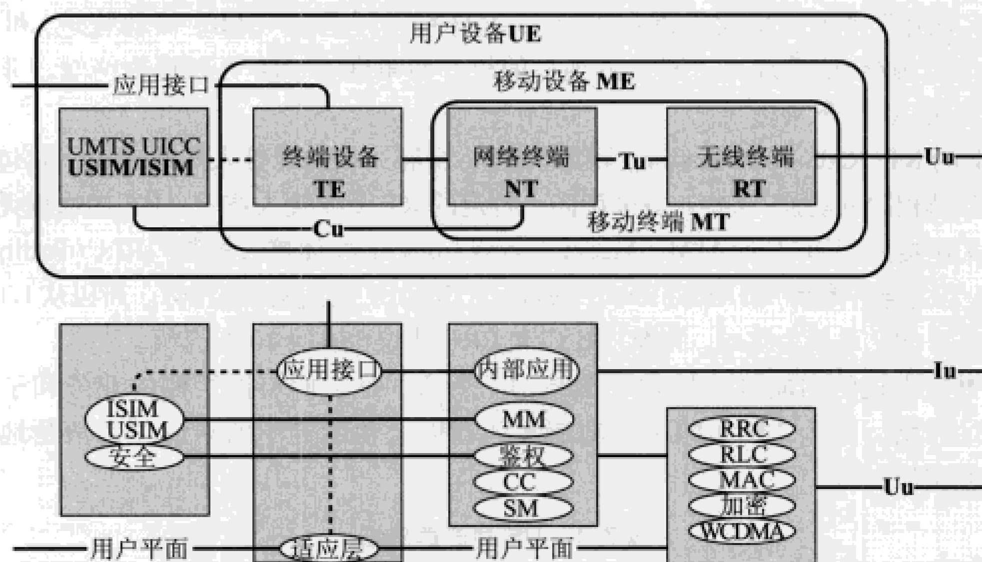


图7.2　UE的主要功能实体分配

严格地说，这里提到的只是核心网中最终的“逻辑”对应体。在有些情况下，实际的协议可能会出于优化的原因而在其他网元处终止。例如，在USIM与HLR之间的移动性管理控制协议经常在拜访网络的MSC/VLR或者SGSN处终止，因为此处一般复制有HLR中的实际信息。

尽管终端结构和网络端的结构互不相同，但有些基本对应的接口在两侧都能识别。两侧所使用的无线接口Uu自然是完全一样的。

在终端侧，Tu参考点（见图7.1）把UTRAN和CN特定部分连接起来，如同网络侧的Iu。由于性能的原因，Tu参考点实际是专有的，它嵌入在UE硬件实现中。而相应的Iu是标准接口，因为UTRAN和CN设备可能来自不同的供应商。

Cu接口对应CN中的D、C、Gr和Gc接口对应，它把交换（MSC和GMSC）或者路由（SGSN和GGSN）服务网络单元连接到归属网络的寄存器网络单元（HLR、AuC和HSS）。这些接口在两侧都是标准接口，这是因为在Cu中有一个运营商和移动设备之间的接口，在网络侧，归属运营商和拜访运营商之间有接口。

7.2 终端的差异

UNTS 终端有多种要求,这些要求不一定相互一致,如图 7.3 所示。这就增加了设备的复杂性,也将影响设备的价格。如果终端的价格太高,它就会增加用户不接受网络实现的风险。图中所列的这些因素以及其他一些因素形成了终端的差异。GSM 市场已经显示出了差异化的发展,一些 MS 型号是针对一般客户的,另外一些型号瞄准的则是商务客户等等。在 3G 中这种差异可能会进一步形成移动终端市场的分割格局。

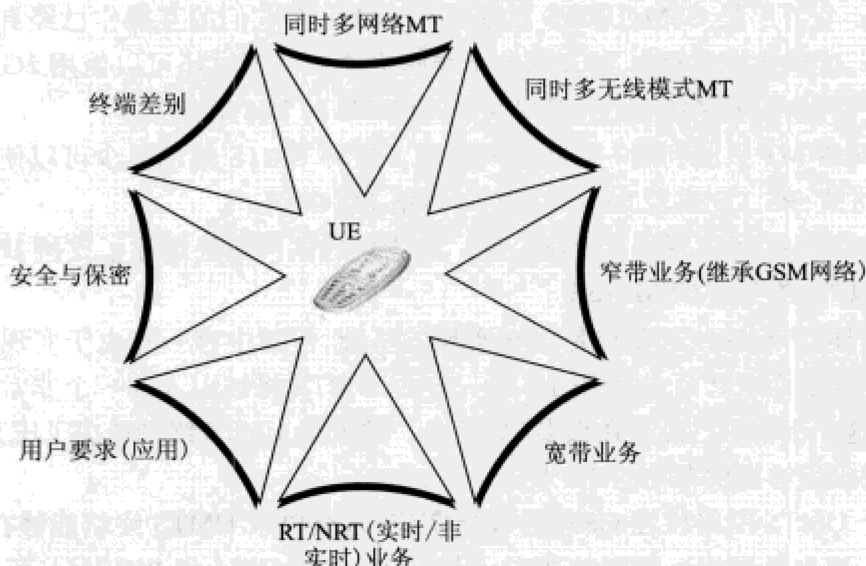


图 7.3 影响 UE 的因素

即使对于最基本的形式,3G 终端的显著特点是它有两个明显不同的服务网络域:用于分组业务的 PS(分组交换)域和用于电路业务的 CS(电路交换)域。在终端来说,这就形成了 3 种不同的操作方式。

- 在 PS/CS 操作方式中,终端连接到 PS 域和 CS 域,并能通过两个域同时提供分组和电路交换业务。
- 在 PS 操作方式中,终端只连接到 PS 域,只通过 PS 域提供业务。但是这并不妨碍在 PS 域提供类似电路的业务。以 PS 业务实现原有 CS 业务的最好例子就是 VoIP。
- 在 CS 操作方式中,终端只连接到 CS 域,只通过 CS 域提供业务。但是这并不妨碍在 CS 域提供类似分组的业务。在 CS 域提供一些实时分组业务,尤其是使用固定比特速率的具有高 QoS 要求的实时业务可能更为切实,尽管它们在外部网络中可能是分组交换的。

在 PS/CS 操作方式中,如果网络支持 MSC/VLR 和 SGSN 之间的可选 Gs 接口,终

端可以优化位置更新过程。在这种情况下，终端可以根据自己的能力选择使用组合的或者独立的更新过程。在组合的位置更新过程中终端只通知 SGSN 新的位置，然后 SGSN 通知 MSC/VLR 更新位置。

移动设备中无线终端功能和网络终端功能的分离使得用户设备可以有级别之分，根据 MT 的功能来使用接入和核心网技术。以下是理论上可能实现的几种基本选择。

- 单无线模式 MT 只能利用一种无线接口来进行用户业务传输。在 UMTS 中，至少在初期这种无线接口是 WCDMA-FDD，这是单无线式 MT 的典型例子。
- 多无线模式 MT 可以使用多个无线终端来进行用户业务传输。其中引人关注的一个情形是 GSM/UMTS 双模终端，3GPP 对它们的互操作已经有明确的定义。这种终端在超出 WCDMA 无线网络覆盖范围时还可以使用 2G 业务。还有一种情形就是能接入 UTRAN 和 GERAN 的 UMTS 终端。
- 单网络 MT 只能利用一种核心网类型。这种 UMTS 终端至少可以使用一种操作方式，PS、CS 或者 PS/CS 就是单网络 MT 的例子。
- 多网络 MT 可以使用多个核心网。最典型的多网络终端除了支持 UMTS 核心网以外，还支持 GSM NSS。

如前所述，所有这些选项都是终端实现的基础，但其中有一些由于实现起来复杂和成本高的问题而缺乏商业吸引力。另一方面，UMTS 将被引入到一个非常成熟的蜂窝市场，在这个市场里已经存在很多 2G 业务。这就给 UMTS 终端造成了压力，从一开始它们就必须能够提供存在的 2G 业务。

第一个 UMTS 网络将在 GSM 的顶层实施，这就要求 UMTS 终端能够在 GSM 网络中漫游。这也是网络运营商的要求，因为可以使用 GSM 和 WCDMA 两种无线接入的终端更有吸引力和使用价值，能从这两个无线接入网络结构中受益。这一要求在电路交换语音业务中尤为适用，因为用户不希望在 UMTS 网络开始安装时由于覆盖限制而造成呼叫中断。所以多无线模式 MT 是扩展网络覆盖范围的一个良好途径。

因此，典型的 UMTS 终端将从多无线模式 MT 和多网络 MT 开始。

这样的 UMTS 终端将为多种业务提供平台。另一方面，用户要求的业务也是多样化的：有些人喜欢传统的语音业务，对先进的流媒体分组交换业务没有兴趣，有些人则认为分组交换业务是必需的。如果终端有能力处理各种业务，其实现将非常复杂和昂贵，当然这样有的用户也就不愿意为那些他们认为是没必要的额外功能花钱。

基于此，我们给出一个大致的描述，它表明了可能出现的 UMTS 终端分割格局。请注意这不代表任何生产商的观点也不代表任何标准，只是为了对移动市场可能出现什么样的分割有一个概念。

在用户及其需求的基础上，并考虑到宽带无线接入所能提供的可能性，我们分 4 种类型来描述用户及其需求和相关业务。

- 传统终端:这和现有的蜂窝手机相当。它制造便宜,因而功能也有限,像电路交换语音接入以及有限的数据接入,其数据速率相对较低,但优于现有的GSM和GPRS。这种终端可以处理GSM和WCDMA无线接入业务,但不一定同时。换言之,它实现了"可选择的多网络MT"。这种终端可看成是一种"GSM的扩展",其使用价值在于现存的GSM网络中,偶尔由于PS连接而使用WCDMA。
- 双模:这种终端类型包括GSM和WCDMA,它可以根据可用的覆盖范围和请求的业务自动选择接入方式。比如,语音呼叫一般通过GSM连接,而数据和多媒体业务通过WCDMA连接。这种终端类型能够利用两种接入的优势,也能够双向完成系统间的切换。系统间切换时,所用业务能自动选择可能的无线接入。因此,这种类型的终端实现了"同时多网络MT"。当UMTS网络广泛投入到商业使用时,这些终端将最可能形成一个大众市场。
- 多媒体终端:这和前面的终端相似,但是从网络的角度讲更智能。双模方式不一定能以最佳方式处理UTRAN无线承载,而多媒体终端能对所用的多媒体呼叫实现"最佳复接"。由此带来的容量节约对UMTS网络的发展非常重要。多媒体终端是蜂窝手机和掌上电脑/笔记本电脑的结合。它包括很多处理多媒体连接和业务的应用。这种终端不一定是面向大众市场的,而是针对商务用户的,至少在初期如此。
- 特定终端:这些终端不一定像以上几种终端那样有"电话参与"。它们集成到其他设备中,有特定的用途。例如这种终端安装在汽车上,和汽车上的计算机协同工作。一旦汽车被盗,这种终端就能"警醒",并能利用GPS和车上计算机的信息指示出该车的详细位置(如街道名)。前三种类型的终端或多或少是按CS/PS操作方式实现的,而这种类型的终端主要使用PS操作方式,其应用范围可以是多样化的。这种应用可以是针对智能家电的,比如让电冰箱根据需要排列食品。在这种情况下,这里所描述的特定终端可集成到通信设备中来建立通信连接。

7.3 终端的功能

UMTS网络预期的生命周期为几十年,因此将会有多种可以兼容但功能不同的终端类型。因此,任意一个终端和任意一个网络都应该能够在某种程度上协商出双方之间可以使用何种可能的基本方式或选择。UMTS采纳了类似GSM的协商机制:网络通过广播大量系统信息向UE通知相关的网络功能,UE知道它本身的功能并通知UTRAN或CN。

有关UE功能的基本信息集称为*移动台类别标记*。随着移动系统技术的演进,类别数量也在增长,因此类别标记的概念也以向后兼容的方式进行了升级。原来的类别

标记大小，早期GSM中使用的最小的classmark1，是2B(1B = 8bit)。Classmark2是5B，classmark3最大可以是14B。Classmark1和2仍用于GSM中。在UMTS中可以把classmark2看成是“CN类别标记”，把classmark3看成“RAN类别标记”。实际要哪个版本的类别标记要看具体情况。一般来说，移动台类别标记3(classmark3)中有关UE基本功能的信息有以下几项。

- 可用WCDMA模式，即FDD或TDD。
- 双模功能，即对不同版本GSM系统的支持能量，支持的频带及其他特征。
- 可用的加密算法。
- UE的测量功能属性，即可以扩展测量功能，执行邻近小区测量时MT从一个无线信道切换到另外一个信道所需要的时间等。
- 使用定位功能以及不同类型定位方法的能力。
- 支持通用字符集2的能力，即称为ISO/IEC10646或Unicode的16bit字符编码标准，而不是短信默认的7bit GSM字符集标准。

除了类别标记以外，还有一个类似的信息单元用来描述UE特定无线接口的全部特性。这个信息单元称为“移动台无线接入功能”。

7.4　UMTS用户

和GSM一样，UMTS也把用户信息从ME中分离了出来。此用户特殊的信息集称为USIM(见图7.4)，也称为业务识别模块(SIM)，因为业务的所有方面都遵循SIM卡中的识别信息。相应信息存储在用户归属网络的HLR中。PS(分组数据域)的用户也可以在UICC中使用附加的ISIM应用而获得IMS服务。相应的ISIM应用信息存储在该用户归属网络的HSS(归属用户服务器)中。

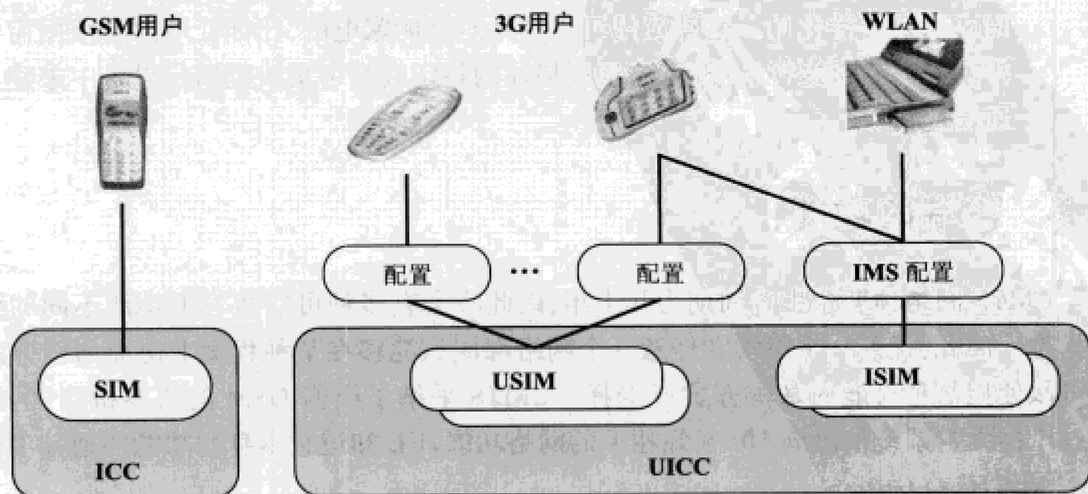


图7.4　GSM和3G的用户识别模块

在 GSM 中,SIM 是一个可移动的集成电路卡(ICC),它是物理存储用户和业务信息的地方。在 UMTS 中,可移动的物理数据存储是 UICC,它包括存有业务信息和识别码的 USIM。可以通过配置或"过滤"访问 USIM,例如这些配置决定了存储信息对用户的显示。配置容易更改:用户能改变其设置,网络也可以更改某些信息。

一个 USIM 可以包括许多不同目的的配置。假定一个用户有两个 UMTS 终端,一个是"传统型"(见 7.2 节),另一个是"多媒体终端"。用户把 USIM 插入任一终端时,用户的入网信息是一样的,但终端的显示信息的方式不同。对于同一用户,针对不同的 TE 采用不同的配置。例如,用户通过"多媒体终端"能够获取的信息(如图片文件)在"传统终端"中是得不到的。

GSM SIM 和 USIM 的明显区别是 USIM 默认方式为可下载的,可通过无线路径读取并更新其信息。USAT(USIM Application Toolkit,USIM 应用工具箱)可以使 TE 应用访问 USIM 信息。

USIM 基本上包括 5 种数据类型。

- **管理数据**:这是由 USIM 厂商以及业务提供商/运营商指定的,不能再改变,比如包括安全算法的密钥、IMSI 和接入类别信息。
- **临时网络数据**:主要是移动性管理信息,比如当前位置区 ID、TMSI 和计算加密时的密钥。
- **业务相关数据**:包括各种业务是否支持,是否被禁用的信息及内部数据。可用业务必须是用户有这样的功能并且经过了许可的。不可用业务表示 USIM 用户不能使用该业务,即使 UE 有这种功能。例如,USIM 可能包含(假设运营商支持)用户本地电话簿、移动用户 ISDN 号、固定拨号号码、业务拨号号码、禁用号码、呼出呼入信息、存储、短信息的状态报告和业务参数、计费提示、具有接入技术的用户和运营商控制的 PLMN 选择器、协作运营商网络列表等。
- **应用数据**:USIM 可根据特定业务的需要而存储少量应用。这些应用可以用 Java 实现,将它下载并存储到 USIM 中,然后在 UE 中运行。
- **个人数据**:用户存储在 SIM 卡上的数据,比如短信息和快速拨号。

这五种类型的数据中,前三类有固定的大小和格式,因为它们在任何 TE 中都必须以同一方式出现,并有基本相同的作用。第四类应用数据还未定义。可以把它当成内存,目前还没有确定这个区域应该多大。第五类原则上有固定的格式,但其大小随运营商和用户而不同:有些 USIM 卡配置了更多的内存用于存储短信息和快速拨号。

对 IMS 用户,可选的 ISIM 应用包括用户安全密钥、IMPI(IP 多媒体个人用户识别码)、IMPU(IP 多媒体公共用户识别码)、识别网络侧入口点的归属网络域名、各种管理数据和控制核实需要的接入规则参考信息。ISIM 的数据内容比 USIM 内容简单,因为 ISIM 不包含与无线或其他具体接入技术相关的信息。基本上,ISIM 需要 USIM 来把分组域接入到归属网络。但如果采用一些补充接入技术(如 WLAN)的话,ISIM 本身就可以实现用户和网络鉴权及密钥协议过程,不需要借助 USIM。

7.5 用户界面

3GPP允许自由设计UMTS终端的用户界面(见图7.5),旨在为终端用户界面提供低成本和创新的方案。

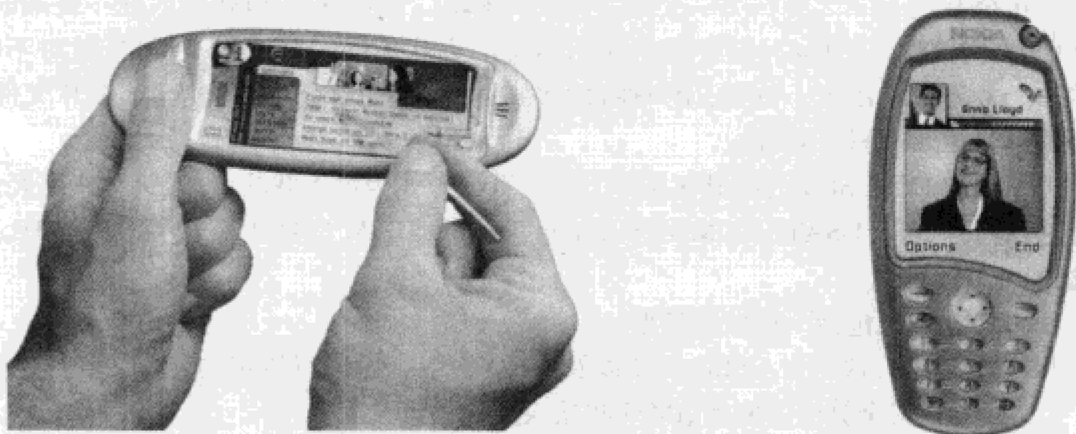


图7.5 概念上的UMTS终端

UMTS终端的用户界面可以遵循GSM终端的"传统"设计,也可以不遵循这种设计。用户界面设计完全取决于终端生产商,但常规数字键盘的设计大都比较相似。

输入和输出的特点是在物理设计上保持最小化,这样就允许有不同类型的UE,并且为容纳以后的发展留有余地。不过,对物理输入要求的最小化使不同UE的控制过程不同,取决于生产商的具体方案。这些要求的共同点是用户的逻辑操作相同。就是说,无论采取什么设计,用户必须提供给呼叫控制和信令传输完全相同的信息。对自动设备也是如此。

有一些可用的和强制的功能是终端必备的,比如"接收"、"选择"、"发送"、"指示"和"结束"。对于管理移动台主叫、移动台被叫及补充业务来说,这些功能是最基本的。这些功能可以按任何一种适当的方式实现,比如传统的数字键盘控制或语音控制等。问题的关键在于用户必须能实现所有这些功能。

"接收"功能用于接收移动台被叫的呼叫。"选择"功能用于输入信息。输入字符0~9、+、*和#的物理方式(也就是"选择"功能)可以通过键盘、语音识别设备、数据终端设备或者其他设备,必须有一种方式能输入这些信息。

"发送"功能负责向网络发送输入的信息(比如被叫用户号码)。"指示"功能提供各种呼叫进程指示。"结束"功能用于终止或者中断呼叫。呼叫的双方都可以执行"结束"功能,另外,也可能因为系统的原因产生"结束"功能,比如没有覆盖或者付费失效。

第 8 章 UMTS 环境下的业务

本章将重点介绍 UMTS 环境下与终端用户和业务相关的问题。首先,我们研究业务范畴:业务是什么,从哪里来,以及业务相关的主要因素是什么?然后,我们将集中讨论业务实现(即业务所要求的技术需求),这种要求称作 QoS(服务质量)。在 8.3 节,我们将会给出一些预期在 UMTS 环境下实现的业务案例。

8.1 业务综述

"业务"这个词源于电信商业领域的膨胀,商业领域几乎在所有情景下都使用这个词。这让每一个研究"业务"的人都感到困惑,尤其是每一个商业体使用这个词时的意思又有些许的差别。在本书中,"业务"这个词采用其原始含义,指网络/运营商/业务提供商向其顾客提供的服务。

第 2 章简述了从 GSM 网络到 UMTS 多址接入的演变。可以看到,随着这种演进,终端用户业务也有很大发展。这就是本节开头所提到的"膨胀":所有的商家都需要拿出一些"东西"来出售,而基本的网络技术已经不是一个问题了。这里需要问以下几个问题。

- 用户真正需要什么?
- 怎样才能从中获取利润?
- 对复杂系统来说,最适当的设计原则是什么?
- 移动网络中和业务相关的因素与固网中的是否不同?

8.1.1 用户真正需要什么

在电信业中,用户期待的并不总是和运营商提供的相一致。一个非常典型的例子是:运营商以为某个技术含量高的全新业务可以成为杀手级应用,但当该业务上市时,运营商才发现,很少人乐意用这项服务。而另一方面,在某些情况下,一些看起来技术含量并不高的业务,可能一下子就走红了。

WAP(无线应用协议)就是一个很典型的不成功例子。WAP 最初基于一个良好的合理想法,它有确切的标准和明确的目标。其想法就是对移动用户开通浏览功能。所

有相关的协议和进程都有规范,以使每一个商业体都能实现该业务于系统中的所有必要的部分。其目标就是用户无论在何时何地都能获得相应信息内容(如号码查询)。那么到底是哪方面出了问题呢? WAP已经注定失败,不再受到公众的关注。

WAP的失败是由多种因素共同导致的。作为一种技术,WAP用于PS(分组交换)信息的传输,但它起初是在CS(电路交换)连接的顶层实现的(即它在GPRS出现之前就发布了)。这样,运营商不得不采用CS数据价格策略,使用户觉得WAP浏览很贵。早期的WAP版本也受到终端开发不统一的影响。作为一种技术,WAP可以让用户传送并且显示图片,可以发送文本和图像,可以处理带有脚本的变化着的内容。所有的这些功能在因特网中都是很基本的功能,用户对信息的显示方式有很明确的期望。当移动终端不能正确地显示内容时,用户就很失望。终端的显示粗糙,颜色丢失,以及有些商家没有完全实现WAP的标准。在有些情况下,这些使得类似的WAP网页在不同的终端上有着不同的显示。

和WAP相反,SMS(短信息业务)却意外地成功了。没有人想到一个简单的、基于文本的链接可以成为杀手锏。但是事情就是这样。到底是什么因素促使了SMS的成功?

首先应该是简单。SMS便于使用,在网络中很容易传输,并且不需要通过极其复杂的VAS(增值业务)设备来处理。用户喜欢一些用起来简单的业务,并且如果他们喜欢,就会经常地使用。当业务相关的信息在网内容易传输时,运营商就不必进行大量投资。其次就是容易理解。当一个业务比较简单时,用户能够理解其功能,他们的期望也比较现实。没有人期待SMS实时传输,大家都知道发送一条短信需要几分钟,有些时候可能更长。当用户习惯了这一传输方式的时候,他们就会尽可能地充分使用这种业务。

人们对SMS成功的例子进行了反复细致地研究。这些研究可以发现一个成功业务(无论它是什么)潜在的主要因素。简而言之就是如下所列。

- 业务必须用起来简单。
- 业务的技术实现必须简单。
- 业务的网内控制功能必须尽可能简单明了。
- 总体的业务功能必须容易理解。
- 业务的价格策略必须遵循该业务的本质。

8.1.2　怎样从中获取利润

从技术上来讲,终端用户的任何需要,无论是现实的还是虚构的,都可以实现。但在现实生活中,必须要考虑的因素就是钱。如果业务开发太贵,或业务实现成本太高,或其价格不能满足终端用户的期望,这个业务在商业上就不会成功,正如先前所述。

正是由于这些原因,电信业务市场是高度划分和专业化的:有提供内容的公司,也有进行内容传输的公司。有些移动运营商自己承担了部分业务,不过由于服务领域的复杂性,业务分割和专业化的趋势已势在必行。

按照这样的业务结构,每一个商业体都能够把精力集中在各自的核心业务上,从

而产生更多的收入。另一方面,这样的业务链可能会在安全和终端用户身份隐私方面带来困难。出于对用户识别的目的,图 8.1 所示的商业体必须在其之间传输保密的数据。最坏的情况是,终端用户的身份信息可能会存在误发送到其他地方的危险。

当然,人们已经认识到了这些关于安全和保密的问题(在第 9 章有详细的论述)。

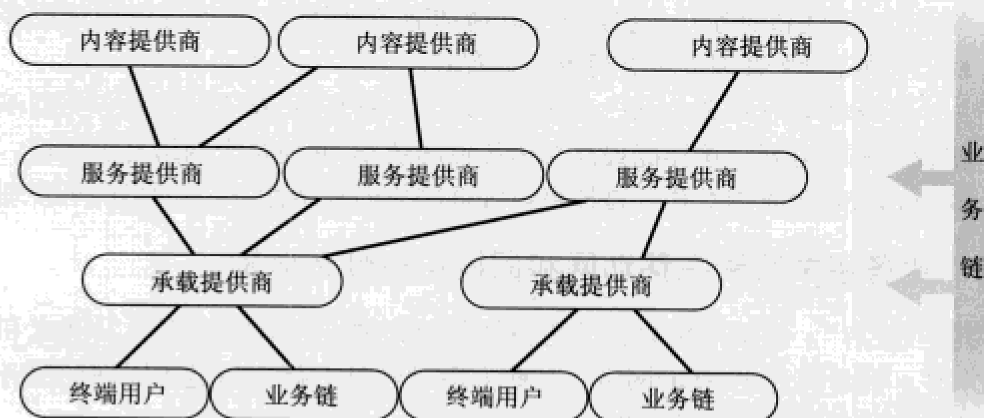


图 8.1 3G 业务及业务/价值链

8.1.3 对于复杂系统,最恰当的设计原则是什么

电信系统一般都有这样一种内在的趋势,就是随着时间的推移会变得越来越复杂。这种发展是多种原因造成的,但是其中有一个原因要比其他原因的总和更重要。

电信系统采用接口开放作为其设计原则,这也给设计过程带来了缺陷。这个缺陷的正式名称就是"后向兼容",即新系统必须尽可能地支持旧的系统和环境。举一个典型的例子,某个移动用户在一个才建 3 个月的现代网络中使用 5 年前的移动终端。旧的终端实际上很可能浪费网络资源,从网络的角度来看,这些设备的运行方式并不是最佳的。对运营商来说,在最坏情况下后向兼容可能非常昂贵,但对终端用户来说,后向兼容永远都是一个预期的、自然的功能。

实现后向兼容通常都会带来许多复杂性,不幸的是,这种复杂性也很容易扩展到终端用户。终端用户下载新铃音就是一个很好的例子。

最初所有的铃音都是单音的,所有的终端都可以处理它。后来市场上出现了和弦铃音,只有某些特定的终端才能处理它。再到目前又出现了真实音调铃音(可以有不同的文件格式),也只有某一些终端类型可以使用。一般来讲,越新的终端功能越强大。最新的终端可以处理所有这三种铃音,而老的终端只能处理单音铃音。假设有一家公司提供这种业务并准备了各种各样的铃声,那么它的历史会是怎样的呢?早期可能只有一两个短信地址,用户能够通过这个地址请求新的铃声,这时的服务既方便又快捷。然后,新的和弦铃声进入市场。公司将面临这样的选择:要么增加一些新的 SMS 入口用于新的和弦铃音,要么改变 SMS 请求的格式。再后来真实音调铃声的出

现也会出现同样的问题。从公司的广告中就可以看出业务复杂性的变化:早期只要一两行加上简短说明就够了,而现在运营商需要列出各种终端类型并说明哪种铃声适用于哪种终端。换句话说,这项业务本身基本是一样的,但内容的变化给接入终端带来了许多必须要克服的障碍,这样就增加了系统的复杂度。

总之,必须要考虑这样一些重要的设计原则。

- 简单性(网络和业务)。这样做可以增加业务使用量,并且可以创造更多的利润。另外,网络管理也将更简单和更有效。
- 一个能承载各种业务的统一的传输网络。也就是说,对不同的业务类型不应当把设备和域分开。这样能提高总体传输的效率,并使整个网络易于管理。
- 最小化网内的控制功能。这样可以降低网络的复杂性,提高网络的可管理性。

8.1.4 业务相关因素在移动网和固网中有什么区别

答案是"没有"。移动网络面临的主要挑战就是要在所有方面都要发展成和固网一样的水平。到目前为止,移动网络在某些方面已经赶上甚至超过了固网的服务。实际上移动网络的主要瓶颈还是带宽。

作为运营商对其网络进行投资的结果,移动接入中传输一个比特的成本并不像固网那么廉价。这一事实必然导致价格方面的压力,终端用户必须面对他们所不希望的费率。固网接入相对便宜,在许多情况下,它只是按月收取固定的费用。移动网络中基本类似的服务并不是采用固定费用,而是根据所传送的比特和分组数据的量来定价,有些情况还要根据所传送的内容定价。换句话说,对于相同的用户和相同的内容,一种接入方式要比另一种更便宜。

对于终端用户来说这种情况通常是不可接受的。这背后的基本问题就是移动网络带给终端用户的增值。需要提出的实际问题是:终端用户愿意为移动性支付多少费用?

8.2 QoS

8.2.1 业务类型和 QoS 属性

8.1.3 节和 8.1.4 节在总体上对业务进行了简要的介绍。本节将详细探讨网络中业务的技术实现。每一种业务都对承载业务信息的传输路径设置了一些要求。有些业务的要求比另一些更为严格。通常情况下,网络要承载许多业务和同时来自多个用户的业务请求。每一个业务都有自己的要求。由于网络资源有限,因此对每一个请求的资源分配目标应当是正好够用,不能太多,但也不能太少。

完全可以给出相当复杂的 QoS 定义,但这样做也将使系统非常复杂。也就是说,复杂的 QoS 分类必然导致复杂的网络,因为这需要在传输业务的实际网络上增加大量的 QoS 控制。

UMTS 引入了一个相对简单的 QoS 概念,它包括四个业务类型和一些用来定义业务类型的业务特征的 QoS 属性。

四种业务类型如下。

- QoS 会话。
- QoS 流。
- QoS 交互。
- QoS 背景。

会话业务类型中目前最主要的是语音电话，不过因特网和多媒体也会引入更多此类的业务，例如 VoIP 和视频会议。终端用户（即通话的人）之间始终保持着实时通信。这是唯一一个业务特性要求严格由人的感知决定的情形。这种业务的主要特征是所传输的信令数据单元（SDU）之间有低的传输延迟和很小的延迟变化。

终端用户视/听实时视频/音频时就需要采用流业务类型。此类业务的特点是以直播方式单向传输到用户。在这种业务类型中端到端数据流的延迟变化必须限制在一个可控的范围内。流业务的接收端一般有一定的时间滞后，终端用户的流应用决定这个滞后量，因此延迟变化的范围也是由终端用户的应用设置的。由于业务是单向传输的，所以相对于会话业务它能容忍更长的延迟和更大的延迟变化。

交互业务类型描述了一种经典的数据通信方案，表现为终端用户的请求——响应模式。消息的目的端，预期在一定时间内会有消息（响应）到达，因此往返时延成为一个关键参数。另一个特点就是数据包的内容应当以低误码率透明传输。

背景业务类型是另一种经典的数据通信方案，总而言之，其特点是接收端并不预期在一定时间之内会有数据到达。因此这种方法多少对传输时间不敏感。另一特点是数据包的内容应当以低误码率透明传输。

上述每一种业务类型相应承载着终端用户的实际业务。表 8.1 是一些典型的业务示例及其业务类型。业务类型的表现是由 QoS 属性定义的。这些可调的参数如下所示。

- 业务类型。该参数的取值为：会话、流、交互或背景。通过分析这种属性，UMTS 可以对业务源作出假设，并对其传输进行优化。
- 最大比特速率（kbit/s）。最大比特速率是用户或应用能接收或提供的上限速率。根据网络的条件，在此速率范围内可以支持所有的 UMTS 承载业务属性。这个参数的目的是限制应用以及外部网络的传输比特速率，使不同工作速率的应用都能达到其最大的用户速率。

表 8.1 业务类型及其特性

业务类型	会话	流	交互	背景
基本特征	• 延迟小 • 延迟变化小	• 中等延迟及延迟变化（由终端用户的应用决定）	• 往返时延是重要因素 • 中等延迟变化 • 请求 - 响应模式	• 接收方（终端用户应用）并不期望响应会在一定时间内发生
业务示例	• 语音、VoIP、视频会议	• 流视频、流音频	• 网页浏览	• 电子邮件及文件下载

- 保证比特速率（kbit/s）。在此速率范围内，UMTS 承载业务属性（如延迟和可靠性）可以得到保证，而超过此比特速率时不能得到保证。保证比特速率可用于基于可用资源的接纳控制，或用于 UMTS 中的资源分配。
- 发送顺序（Y/N）。此参数表明 UMTS 承载是否应当按顺序发送 SDU。这个参数来自用户协议（PDP 类型），说明是否接收乱序的 SDU。乱序 SDU 是要丢弃还是重新排序主要取决于特定的可靠性。注意对 PDP（分组数据协议）类型（IPv4 或 IPv6），发送顺序应设置为“N”。
- 最大 SDU 大小（字节）。该参数定义了最大 SDU 大小，在最大 SDU 大小情况下，网络必须满足所协商的 QoS。最大 SDU 大小用于接纳控制以及传输的策略和优化。对于超过此大小的包的处理与具体实现有关，例如被丢弃或在降低 QoS 要求下继续传输。
- SDU 格式信息（比特）。借助此参数可定义出所有可能的 SDU 大小。其原因是 RAN（无线接入网）在透明 RLC 协议模式下需要 SDU 大小信息，RLC 无重传时这个信息对频谱效率和延迟有利。因此，如果应用能指定 SDU 大小，承载将会更加经济。
- SDU 错误率。该参数指示 SDU 丢失或检测出错的比例。SDU 错误率是针对相容（conforming）业务定义的。通过保留资源，SDU 错误率性能和负载条件无关，而在不保留资源的情况下，例如在交互和背景业务类型中，SDU 错误率作为目标值使用。此参数用来配置协议、算法和错误检测方案，主要用在 RAN 中。
- 残余误比特速率。此参数指示发送的 SDU 中未被检测出的误比特速率。如果没有错误检测请求，残余误比特速率将表示发送的 SDU 中的误比特速率。该参数用于配置无线接口协议、算法和错误检测编码。
- 错误 SDU 传输（Y/N/ - ）。该参数指示被检测为错误的 SDU 是应该发送还是应该丢弃。“Y”表示采用了错误检测并且错误 SDU 连同错误指示一起发送。“N”表示采用了错误检测并且丢弃错误的 SDU。“ - ”表示不考虑错误检测直接发送 SDU。
- 传输延迟（ms）。该参数表示在一个承载业务时间以内，已传送 SDU 的延迟分布中占 95% 的最大延迟。SDU 延迟定义为从一个 SAP 发出请求到发送至另一个 SAP 的时间。此参数与具体运用所能承受的延迟有关。结合 SDU 误码率参数，当应用要求所有发送数据包的 99.9% 都在某一特定的时间内进行传输时，导出 95% 处的值时需要加以注意。此参数允许 RAN 设置传输格式和 HARQ 参数。
- 业务处理优先级。该参数表明 UMTS 承载的 SDU 相对于其他承载的重要性。交互业务尤其需要对不同的承载质量进行区分，这一点正是通过业务处理优先级来实现的，该参数可使 UMTS 相应地进行业务调度。按其定义，“业务处理优先级”是绝对保证参数的替代，因此这两个参数不能用于同一承载。
- 分配/保留优先级。相对其他 UMTS 承载，该参数表明分配和保留 UMTS 承载

时的相对重要性。分配/保留优先级属性是一个不受移动终端协商的用户属性，用于执行分配和保留时区别不同的承载。在网络资源不足的情况下，相关网元在实现接纳控制时优先处理高优先级的承载。

- 源统计描述符（"语音"/"未知"）。该参数说明 SDU 数据源的特征。会话语音遵循已知的统计特性，或者有不连续的传输（DTX）因子。如果 UMTS 承载的 SDU 来自语音源，那么 RAN、SGSN（GPRS 服务节点）、GGSN（GPRS 网关节点）以及 UE（用户设备）可根据经验计算出统计复用增益，用于相关接口的接纳控制。
- 信令指示（Y/N）。该参数表明提交 SDU 的信令特性，是不覆盖其他 QoS 的额外属性。仅用于交互业务类型。如果信令指示设备为"Y"，则 UE 应将业务处理优先级设置为"1"。此时信令业务将和其他交互业务有不同的特性，例如更高的优先级、更低的延迟或更高的峰值。该参数可使 RAN 的运行相应增强。用于 IMS 的信令业务是信令指示的一个例子。由消息的 QoS 信息单元中的 UE 发送信令指示。

QoS 参数组合的技术实现称为"承载"，它形成了具有一定特性的某一业务类型。承载是已分配网络资源的集合，它形成了一个能实现 QoS 要求的"比特管道"，是终端用户业务请求的响应。

图 8.2 给出了承载利用这些参数及其组合的方法。实际业务的要求出现在 UMTS 承载处，终端内的本地承载保持相同的定义。如果连接超出网络，业务请求就由外部承载的定义来满足。注意外部承载的定义和 UMTS 标准不一样。这可能会引起一些业务的问题，因为 QoS 在 UMTS 网络之外不一定能得到保证。

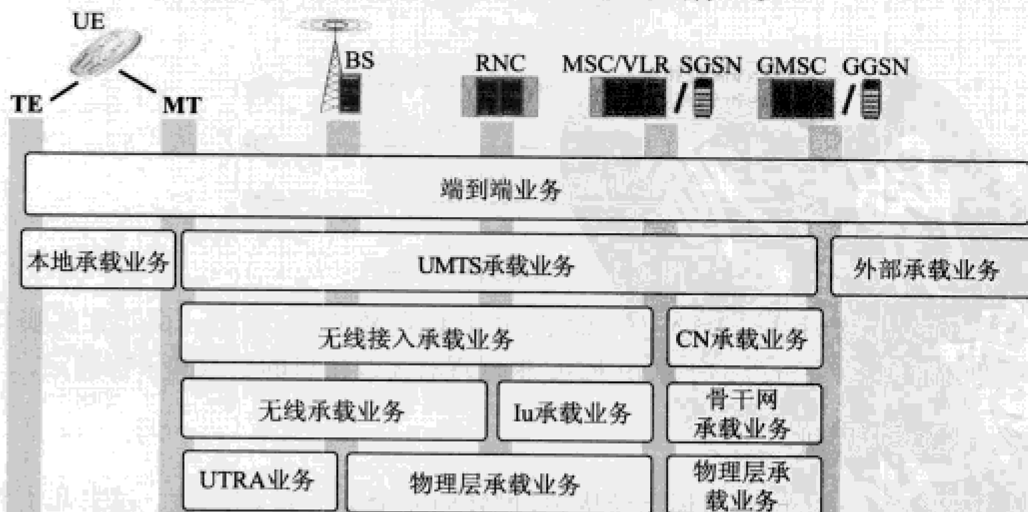


图 8.2 UMTS 系统中的承载/QoS 结构

UMTS 网络是由特性不同的许多部分构成的,系统的这些部分也必须由不同的承载覆盖。覆盖系统某一部分并且靠近物理层连接的承载对 QoS 有更严格的要求。例如 UMTS 承载的传输延迟是以毫秒级定义的,而在 UTRA 业务中是以微秒级定义的。这是必要的,否则原始的 QoS 要求就可能不能实现。

回顾第 5 章提到的 AC(接纳控制)和分组调度机制,RNC 在考虑 QoS 时起着核心的作用。在 QoS 意义下这个过程称为承载管理(如图 8.3 所示),指系统实际如何处理这些参数的整个过程。

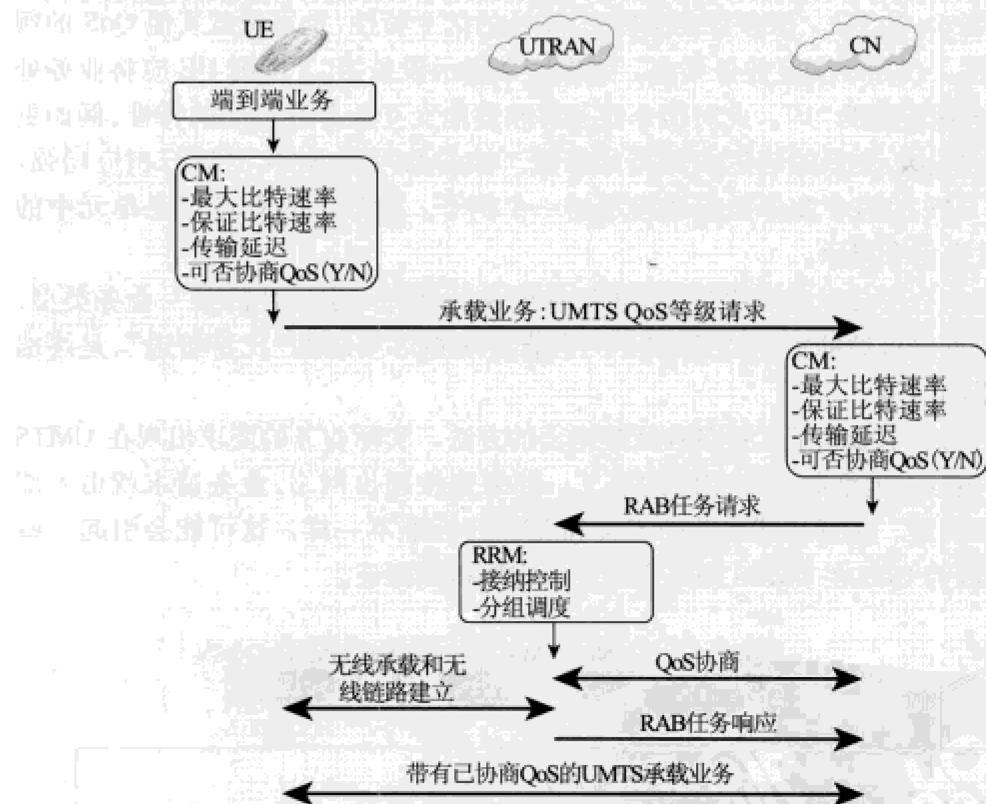


图 8.3 承载管理的原理图

对承载的最大限制在用户入网时设定,并由 CN(核心网)管理。由于无线接口是最有可能的瓶颈,实际分配的承载由 RNC 根据现有无线接口的负载和干扰确定。

8.2.2 QoS 机制

从 3GPP R5 颁布开始,目标已经从 3G 网转向完全基于 IP 的网络。过去几十年的经历已经证明了 IP 的数据传输概念。尤其适合于连接质量为"尽力"型的网络。按这种方式运行的最出名的网络就是公众因特网。

随着整个世界向移动性发展,电信和数据通信融合的实现,传统 IP 的尽力方式遇到了新的挑战。IP 起源于数据通信,在那里的大多数情形可以满足于"尽力"。在移动网络中,终端用户已经习惯于有明确的数量和质量特征的面向连接的服务。这样给在

标准 IP 顶层设计 QoS 保障机制带来了难题。

在系统中引入 QoS 最直接的方法是让终端用户拥有无限可用的带宽。该方法称为“过量配置”。靠过量配置来保证 QoS 是非常昂贵的，为此，针对宽带资源有限、用户数量持续变化的环境，人们进行了大量的标准化工作以寻求一种替代的 QoS 保障方式。

后续的几个小节将简要介绍其中的一些机制及其一般性原理。注意我们所列出的只是一部分，但在 QoS 方面，它们是最普遍的方法，也是 3GPP 中的研究内容。

8.2.3 RSVP

RSVP 可能是 QoS 提供机制中最复杂的一个，但它确实提供了模拟 CS 连接的可能性。RSVP 实际是用来实现综合业务的。综合业务是一种实体，包含以下两种选择。

- 确保：这是一种效仿专用虚拟电路的综合业务状态。它可以根据议定的业务参数在端到端连接上提供稳定的延迟范围。
- 受控负载：这种综合业务状态与“无负载条件下的尽力业务”的意义相同。换句话说，它比“尽力”要好，但这种优越性并不能在所有条件下都得到保证。

如图 8.4 所示，发送端（业务）按带宽限制（最大和最小）、延迟和抖动来描述外出的业务。通过 PATH 消息中的 RSVP 将这些信息发送到接收机地址。路由中每个支持 RSVP 的路由器接收 PATH 消息及其参数，建立一个路径或者确切说是一个路径状态，它总包括 PATH 消息来自的那个前一地址。最后，PATH 消息到达接收机（业务）。

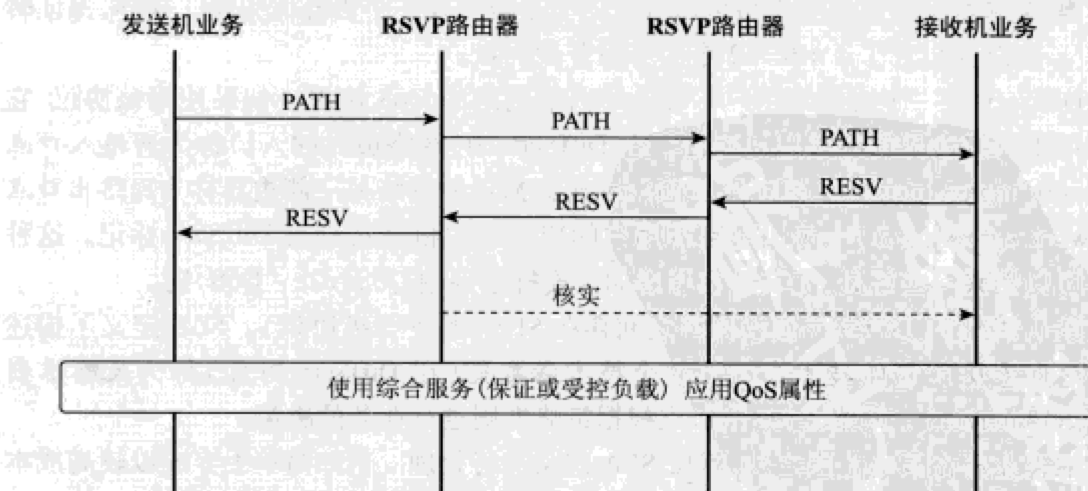


图 8.4 RSVP 主要原理

为了保留资源，接收机（业务）发送一个 RESV 消息到发送机（业务）。该消息包含 PATH 消息的初始 QoS 属性，还包括一个定义了综合业务类型的“请求说明”。RESV 消息也包含数据包过滤信息（传输协议和端口号）以对这些数据包进行保留。所有这些定义一起形成了“流描述符”，路由上的每个 RSVP 路由器用它来识别资源保留。

RSVP 路由器收到 RESV 消息后启动 AC 和其他访问进程来鉴别请求并分配所需的资源。例如,如果不能分配资源,路由器发送错误信息到前一地址。如果所有相关的 AC 过程都成功,RSVP 路由器就发送 RESV 消息到下一路由器。

最后一个 RSVP 路由器接收到 RESV 消息后发回一个确认消息到接收机(业务),表示业务通路已经准备好,并能达到所要求的 QoS 特性。这里所说的最后一个路由器可能是指离发送端(业务)最近的 RSVP 路由器,也可能是多播流情况下的公共保留点。

发送端(业务)和接收端(业务)之间的路由可能包含 RSVP 路由器和非 RSVP 路由器。此时非 RSVP 路由器是透明的,即 PATH 和 RESV 消息通过这些非 RSVP 路由器时不进行处理。注意这种情形下的非 RSVP 路由器形成了一定的风险,因为不确定它将怎样对相关的连接进行资源保留。

8.2.4　区分服务

正如其名,DiffServ(区分服务)是一个相对简单的方法,它把业务进行分类,然后在网络之中区别对待这些类型。DiffServ 可以有许多不同的业务类型,但只有两种非常重要的业务等级或业务类型。业务类型事先定义的行为模式和限制,称为*代码点*(codepoint)或 DiffServ 值。

- *加速转发*。这一类型把延迟和抖动降到最低,因此有最高等级的 QoS。任何不适合类型定义的业务都简单丢弃。加速转发实现单一的区分服务代码点。
- *保证转发*。该业务类型可以分成四个子类型及三个丢弃优先级。这样,保证转发总共包含了 4×3=12 个区分服务代码点。

DiffServ 是一个对终端用户不可见的内部网络的 QoS 协议。如果使用该协议,它将应用于网络边界的终端用户连接。在 DiffServ 中,网络边界的入口称为*网络入口点*(network ingress point)。相应地,DiffServ 定义撤消的网络另一侧边界称为*网络出口点*(network egress point)。可以对终端用户的应用或主机直接进行 DiffServ 标记。这种方法可以带来一些好处,尤其是在考虑如何安排端到端 QoS(e2e-QoS)时。

默认情况下,DiffServ 假设网络之间存在 SLA(服务等级协议)。SLA 定义了描述网络之间连接质量的技术参数。这个技术参数集(在 DiffServ 方面)称为*策略准则*(policy criterion)。网络入口/出口点根据策略准则进行业务的决策。

如果业务在策略范围之外,就按 SLA 定义进行处理。例如简单丢弃或以较高成本发送。业务策略定义和 SLA 可以基于时间、日期、源或目的地址、应用 ID 值等。

图 8.5 示出了基本 DiffServ 的原理以及多个网络互相有 SLA 时的应用。如果 DiffServ 标记是在用户/主叫端实现,那么 SLA 对该入口点或/出口点也有影响。如果用户/主叫端是 ISP,这些点一般采用原来的 SLA。如果用户/主叫方是移动用户,SLA 实际称作"定制"。定制并不一定表明是否应用了 DiffServ,但拥有合法捆绑的定制可使运营商保证一定的业务等级,这种关系和 SLA 很类似。

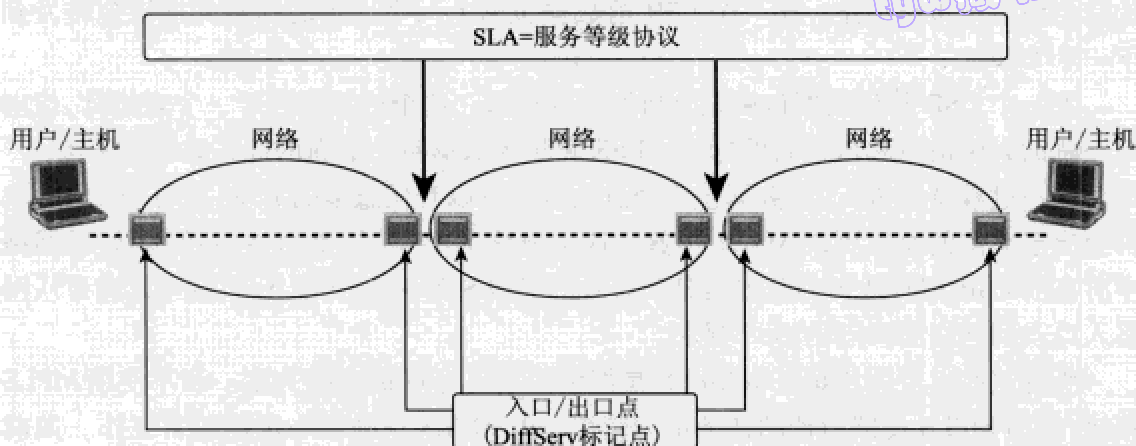


图 8.5 DiffServ 原理图

8.2.5 MPLS

MPLS(多协议标签交换)与 DiffServ 有许多共同的特点。比如说,MPLS 也在网络入口/出口点标记业务。但 MPLS 与 DiffServ 提供的范围不同:DifferServ 在整个网络上对业务分类,MPLS 只在下一个路由跳上进行业务分类。

MPLS 不受任一应用的控制(它没有应用可编程的接口即 API),不包含终端用户/主机,它仅存在于服务器中。

需要注意的一个特征是,MPLS 与协议无关,它可以应用于任何网络协议。IP 当然是首选的,但也可以是 ATM 和帧中继。在"MPLS 框架"环境中,MPLS 还可以直接用在数据链路层的顶端。

图 8.6 示出了网络中 MPLS 的基本原理。

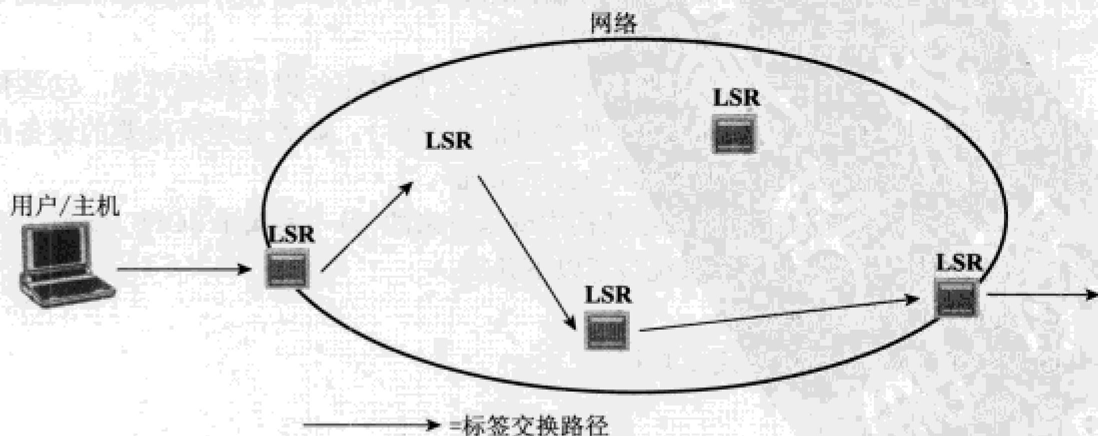


图 8.6 MPLS 原理图

支持 MPLS 的路由器称为 LSR(标签交换路由器)。MPLS 网络中的第一个 LSR 接收数据包,并根据包的目的地址或包头中的其他信息作出转发决定。用于转发决定

的信息由本地策略决定。第一个LSR给数据包贴上一个适当的标签并把该包转发到下一个LSR。

下一个LSR收到数据包后先分析所贴的标签。这个标签相当于一个表指针,指向下一跳的索引信息和该包新的标签。LSR再给该数据包贴上新的标签后继续发送。

这一过程持续进行,在数据包所经过的链中可以有任意多的LSR,在每个LSR中,都会出于路由的原因更改MPLS标签。这个链称为LSP(标签交换路径)。如果网络中所有的LSR都有适当的配置信息和有效的MPLS路由表,那么LSP就可以满足从网络入口点到网络出口点的QoS要求。

所有这些以及图8.6说明MPLS是网络中实现QoS的直接方案。和不使用MPLS相比,使用MPLS使路由器的任务更为简单。但MPLS单独不一定能正常工作。如前所述,每个LSR有自己的索引表指向下一跳及其标签。前一LSR查表决定下一跳。为了保证QoS,表的内容必须准确。如果网络包括很多LSR,表的数量也会随之增加。此外,在一个较大的MPLS网络中,如果有一个LSR发生改变,就需要对大量的表进行更新。因此MPLS另外需要一个协议/机制来保持LSR表的更新。基于此目的有一些可选的方法,一种方法就是LDP(标签分配协议),另外一种方法就是RSVP和MPLS相结合。

8.3 业务子系统

到目前为止,我们已经介绍了业务、技术质量要求及其实现可能性的背景知识。本节将简略介绍UMTS网络可能提供给终端用户的业务。

引入3GPP R5时的一个目标就是想让传输网络更为通畅,给业务实现留出更多的"空间"。换句话说,如果业务可以确信传输网络是统一的,那么业务结构和功能就不会对网络市场上各种各样的传输方式加以限制。

UMTS网络的一个主导原则是网络的主要任务是为业务提供传输资源。这些传输资源应能完成业务设置的质量要求(如本章前面所讲)。业务处理所需要的设备位于传输网的顶层并形成了自己的实体"业务子系统"。

有些业务子系统是从先前的网络结构中继承下来的,另一些属于3GPP R5所引入的新的网络实体。这样,业务子系统包括以下几项。

- 从GSM中继承的业务。
- USAT(UMTS SIM应用工具箱)。
- 浏览功能。
- LCS(定位业务)。
- IMS业务机制,它包含以下两项。
  - ○短信业务。
  - ○呈现业务。

8.3.1 从 GSM 继承的业务

UMTS 有 GSM 的背景，是移动网络中的重大演进，所以它基本支持标准 GSM 定义和支持的所有业务。尤其是 3GPP R99 实现的应用，它实际上是基于 GSM 的实现直接提供更大的带宽和更高的终端用户数据速率。

自 3GPP R4 以来，情况就有了不同。3GPP R4 通过在 CN 中引入 MGW（媒体网关）和在网络结构中引入 MSC（移动交换中心）服务器单元带来了容量和呼叫控制的可扩展性。3GPP R5 的目的是在 CN 内统一传输网，业务接口在某种程度上也必须改变。由于后向兼容是电信中的一个问题，所以在 3GPP R5 中集成新业务时必须要认真考虑。

作为 3GPP R5 标准（TS23.002v.5.12.0）及后向兼容两者的结果，R5 网络继续支持 CS 业务和 PS 业务。但是重点已经转向了 PS 业务，并且 PS 域包含了用于 IMS（IP 多媒体子系统）的新接口，这样就为未来的业务创造了平台。

图 8.7 示出了继承 GSM 的 CS 业务的高级连接性与域级的 3GPP R5 结构之间的比较。由图 8.7 可知，CS 业务采用 CS 域进行连接，CN 通过 GERAN（GSM/EDGE 无线接入网）或 UTRAN（UMTS 陆地接入网）进行接入。GSM 终端很自然地代表利用 GSM 继承业务的主要终端部分。它们通过 GERAN 接入 UMTS 网络，网络需要保证业务级别等同于其在 GSM 中的级别。



图 8.7 3GPP R5 中从 GSM 继承的 CS 业务的连接性

图 8.7 中通过 UTRAN 的黑线分支表示可能来自于实际 UMTS 终端的 CS 业务。这种情形对应网络只是部分实现了 3GPP R5，其他部分仍遵循 3GPP R99 的功能原则。在 3GPP R99 中，QoS 会话级业务使用 CS 连接。

图 8.7 典型的代表业务就是“话音”，更正式的叫法是电话业务 TS11“语音”。

从 PS 继承的业务称为“2G GPRS”，UMTS 也应支持该业务。GSM/GPRS 终端使用 2G GPRS（通用分组无线业务），通过使用该业务终端用户能够建立“尽力”型 QoS 连接，而不需要任何确切的质量保证（如图 8.8 所示）。

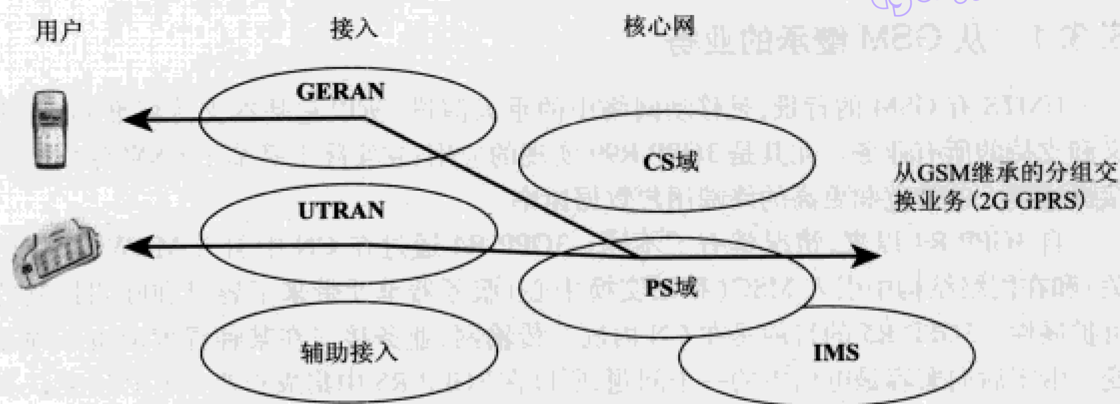


图8.8 3GPP R5中从GSM继承的PS(分组交换)业务的连接性

2G GPRS用于消息和浏览应用(如SMS和MMS)。从原理上来讲2G GPRS也可以使用IMS业务,但接入IMS之前,2G终端需要添加一些附加的应用。

8.3.2 USAT

USIM(UMTS SIM)卡在物理上类似于GSM的SIM(用户身份模块),但USIM卡有更先进的特性。USIM有更大的内存空间、更强的处理能力,并且可以下载。这就可以带来GSM系统中不一定有的新型业务。注意USIM后向兼容GSM SIM卡,但不是在所有条件下都保证兼容。

USAT(UMTS SIM应用工具箱)是一个独立的平台,它包括操作USIM所需要的工具(如图8.9所示)。

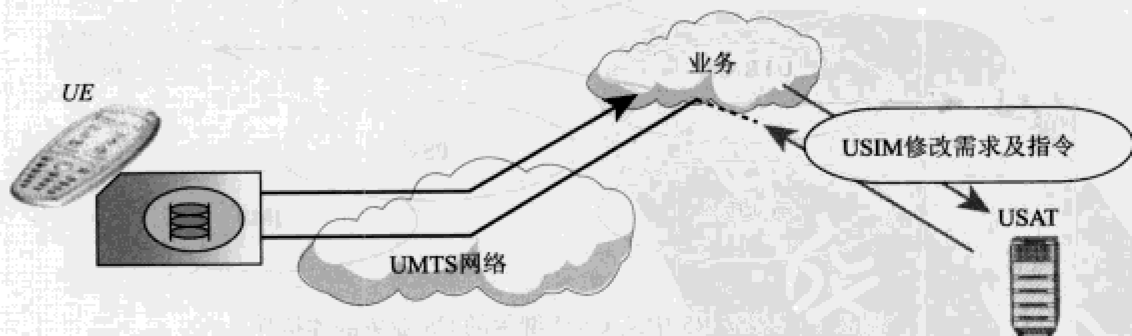


图8.9 USAT原理图

运营商可通过USAT提供能对终端菜单结构进行修改的业务。这样运营商就可以建立便捷的"单键"浏览接入,进而使同一运营商或特定业务提供商提供更多的业务。8.8.3节将简要介绍这种移动浏览技术。

USAT是一个非常强大的工具,运营商可以彻底地改变用户入网的所有参数,如IMSI号。有些业务需要这样的功能,但因为风险高一般不推荐使用。

8.3.3 浏览工具

根据移动浏览器所暗含的意思，移动浏览器是移动设备中的一个应用，其主要功能是在显示器上显示内容、根据用户的请求与显示的内容或程序内容进行交互，从请求的位置获取新的内容。听起来好像很难，实际上并不难，因为我们中的大多数人多年来一直都在通过传统的因特网使用浏览应用。本节简要介绍当我们把移动性加到浏览上时所发生的事情和将要发生的事情。

从终端用户来看，浏览器提供了一种接入业务的方法，这些业务在移动网络中或者需要通过移动网络。终端用户需要理解一些基本的概念，所幸这些概念大部分和传统因特网一样。它们是：浏览器（应用）、网页、地址和链接。这些概念都是一些浅显且熟悉的词，所以我们不做进一步的解释。相反，记住经常应用于浏览和与接入类型无关的内容的一些原则是很有帮助的，这些原则有以下几项。

- 业务概念必须易于理解。业务必须是许多交互网页的简单组合，它们共同形成了终端用户业务。
- 新业务的增加必须简单。如果每个新的业务都需要终端用户安装新应用很明显是失败的。相反，新的业务应当通过新的地址获得。
- 业务必须使用标准的接口单元。由于业务之间差别很大，所以业务之间的接口应该具有固定的特性，总按预期的方式出现（如启动应用的位置、链接的样式、关闭应用的位置等）。
- 丰富的视觉效果。浏览业务应该包含可视单元，而不是纯粹的语音或文本。这一特性和终端的发展紧密相关。

为了技术上处理这些特性，移动浏览应用必须相对复杂，能处理各种媒体类型。图 8.10 粗略地示出了移动浏览应用的大致原理。

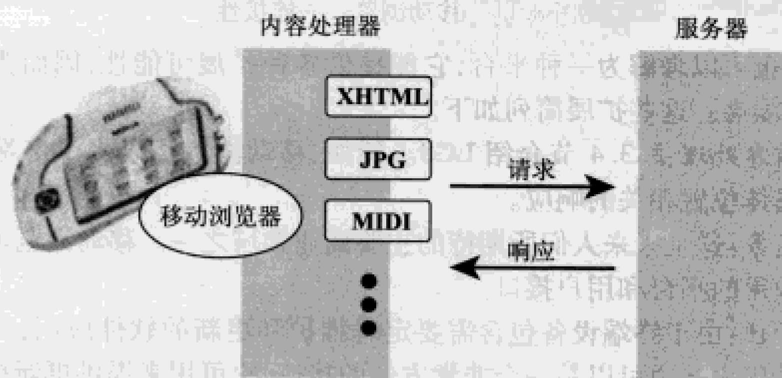


图 8.10　移动浏览的大致原理

终端用户所看到的页面是采用浏览器可以正确显示的标记语言编码的。目前，这种标记语言为 XHTML（Extended Hypertext Mark-up Language，可扩展超文本标记语言），它包括 WML（无线标记语言）和 HTML 定义。采用 WML 的 WAP 技术存在一些

严重局限性，它影响终端用户的浏览体验，这一点促使移动浏览器标记语言需要更完整的解决方案。

使用 XHTML 描述的页面可以有全部的内容形式：纯文本、图片和语音等。文本部分由 XHTML 来处理和描述，但图片的分辨率及其他相关问题由更合适的独立处理器处理，以保证最好的视觉效果。语音部分的原理也如此。如图 8.10 所示，这里有很多内容处理器并且其数量还可能会增加。图像就是这种使用的一个很好的例子：因特网目前可以支持几十种可用的图像格式，所有的这些格式都需要展示给终端用户。最常见的图像类型有：BMP（位图，存在多种不同的 BMP 子版本）、JPG（用于照片，存在多种版本）、GIF（为网页裁剪的照片格式，存在多种版本）、TIFF（高分辨率图像格式）和 PNG（标准浏览器支持的便携网络图像）。

从网络的观点来看，移动浏览是一种基本的业务功能，它对传输网络自身没有太多的要求，因为移动浏览主要属于终端的范畴。在移动浏览中，网络任务是可以使用的，并能按照终端用户定制的以浏览为目的的 QoS 定义打开数据连接（如图 8.11 所示）。

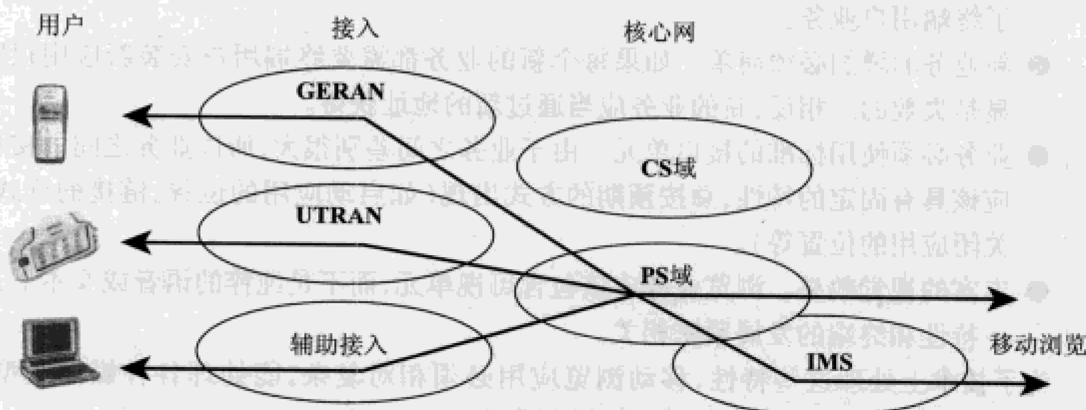


图 8.11 移动浏览——连接性

移动浏览也可以理解为一种平台，它能提供各种扩展可能性，因而为进一步开发业务提供了可能性。这些扩展简列如下。

- 定位信息处理：8.3.4 节介绍 LCS。例如，移动浏览可以提供终端用户的请求与其具体位置相关的响应。
- 移动商务：这是未来人们所期待的主要商业领域之一。移动浏览可以作为电子商务应用的平台和用户接口。
- 设备管理：由于终端设备包含需要定时维护和更新的软件应用，所以移动浏览对终端用户来说可以是一个非常方便的接口，它可用来提供更新机制并支持对终端的配置。注意这样的开发可能对安全有影响。
- 业务发行和安装：使用移动浏览，运营商可以就新的业务向终端用户提出建议或进行广告，并提供快速业务激活机制。
- 新 XML 内容类型：当使用多媒体的业务最终出现后，需要能够向用户提供新的内容处理器以显示新类型的内容。

- 离线浏览：终端不需要一直都连线到网络，有些业务是可以离线使用的。移动浏览可以提供这类业务。这一点基于 XHTML 的可下载业务分组，业务或其相关部分可以下载到终端后离线使用。
- 语音浏览为标准的"链接单击"替换为语音命令提供了可能。还可能让接收到的内容是可听的而不仅仅是可视的。
- 语义网是未来因特网的构想，其内容不再局限于显示媒体。语义网可以调整请求的信息，使其能自动适应各种终端。对移动用户来说有很明显的优势：请求的内容都会以最佳的格式返回，从而达到更好的浏览体验。

8.3.4 LCS

移动定位将成为未来蜂窝系统中的重要特点。LCS(定位通信服务)演进的途径主要有两种：一种是根据无线小区的覆盖得到近似定位信息，进而得到精确的定位信息；另外就是利用 GPS 的精定位信息，或者采用无线网和向移动电话发送的辅助数据采用基于时间的高级计算方法来得到位置信息。

基于定位的商业应用很多，如舰队管理、交通息管理、运输、就近服务、紧急服务、导航服务和游戏等。另一个例子是网络运营商采用基于位置的负载信息对移动系统的性能和容量进行规划和优化。

蜂窝技术允许终端用户移动，无论他/她移动到何处都可以使用各种各样的通信服务。不过这种移动的自由性也对用户进行准确定位制造了难度。

本节先介绍目前移动网络中已采用的几种不同的定位方法的基本原理。然后介绍 UMTS 所指定的定位方法。进而深入讨论 UMTS 的定位体系结构和分配给不同网络单元的定位功能。位置信息也可以直接在移动电话和定位服务器之间通信，在 8.3.4.5 节中将介绍这种类型的方案。

为了保持与 3GPP 标准中术语的一致性，我们使用"position"一词作为无线网络中的通用概念，但是当涉及定位信息服务方面时，则使用"location"一词。在 3GPP 及其规范中所指的整体概念称为 LCS(Location Service，定位服务)。

图 8.12 给出了 3GPP R5 网络中的接入网、核心网域和 LCS 连接。

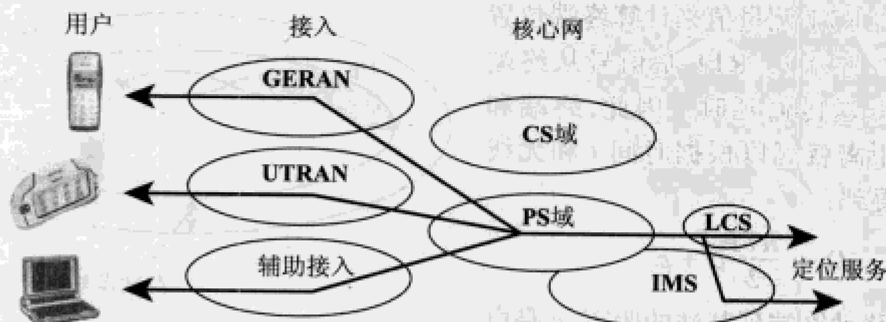


图 8.12 3GPP R5 中 LCS 连接

8.3.4.1　定位方法概述

为了确定蜂窝网络中的移动电话的地理位置，人们调查和研究了许多定位方法。最重要的方法有以下几项。

- 基于小区覆盖的定位。
- 基于RTT(往返时间)的定位。
- TDOA(到达时间差)定位。
- E-OTD(增强的观察时间差)。
- GPS(全球定位系统)。
- TOA(到达时间)定位。
- AOA(到达角度)定位。
- RNBP(基于参考节点的定位)。
- 伽利略定位系统。

下面几节将介绍这些方法用于UE定位的基本原理，并简单分析它们能够达到的精度。3GPP R5对基于小区覆盖的方法、TDOA(3G)、E-OTD(2G)和基于GPS方法进行了标准化，因此这里对这些定位方法的介绍更详细一些。

8.3.4.1.1　基于小区覆盖的定位

发现终端驻留的小区或者最近驻留的小区就可以估计出终端的位置。无线网络控制器(3G中的RNC)、基站控制器(2G中的BSC)或独立的SMLC(服务移动定位中心)估计出相应指示小区的近似地理坐标，并把结果发送到网络中的定位服务器。

注意在3G标准中，小区的实际标识看作是无线信息，所以可能不会传输到CN中。而是将小区ID映射为“业务区域识别”，它可以发送给CN。

小区的覆盖范围或大小与无线信道的特性和无线网络规划策略有关，因此对某些基于位置的业务来说，按小区覆盖定位的方法不能满足定位质量的要求。因此这种该方法一般都和RTT定位方法(也叫TA定位方法)结合使用以更精确地决定终端坐标。

8.3.4.1.2　基于RTT的定位

无线信号的RTT也可以用来增加位置估计的准确性。可以使用几个BS(基站)的信号分支的RTT测量值来计算终端位置(如图8.13所示)。RTT是信号从终端到基站的往返传输延时。因此，终端和基站间的距离就可以根据时间t和无线电波速c得到：

$$D = \frac{RTT}{2}c + \varepsilon$$

其中D是移动终端到基站的距离，c是电磁波的速度，在自由空间中等于光速(3×10^8m/s)，RTT是往返时间，ε是测量误差。

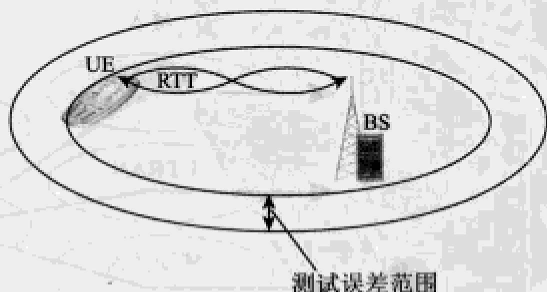


图8.13　基于RTT的定位

注意距离 D 实际代表以 BS 为中心的一个圆周的半径。因此，如果可能的话，可以用邻近基站的 RTT 测量值更准确地估计出移动终端的位置。此时估计的位置是三个相邻圆的交点，这三个圆分别以各自的基站为中心。最终的位置估计精度由 RTT 测量的误差范围决定。

8.3.4.1.3 TDOA 定位

TDOA 方法的基本原理和 TOA 不同（见 8.3.4.1.5 节）。在 TDOA 方法中，终端观察周围基站无线信号的 TDOA，通过处理终端和至少三个基站的 TDOP 测量值来估计未知的终端位置，它至少需要三个已知坐标的基站。终端测量的 TDOA 由两部分组成：

$$TDOA = RTD + GTD$$

其中，GTD（Geometric Time Difference，几何时间差）源自几何学，指手机到两个基站之间的传输延迟差。GTD 在两个基站之间建立了一个双曲线，因此手机的位置信息包含在 GTD 中。另外，在 WCDMA 等系统中基站不是同步的，所以必须已知 RTD（Relative Time Difference，相对时间差）。RTD 是相邻基站发送信号的时间差。

图 8.14 示出了 TDOA 定位方法的原理。终端的位置根据服务基站和邻基站之间的 TDOA 计算，TDOA 确定了一条双曲线，其焦距就是相应基站发射天线的坐标。如果两个以上的 TDOA 值可用，终端的位置可利用双曲线的最小二乘距离来估计。

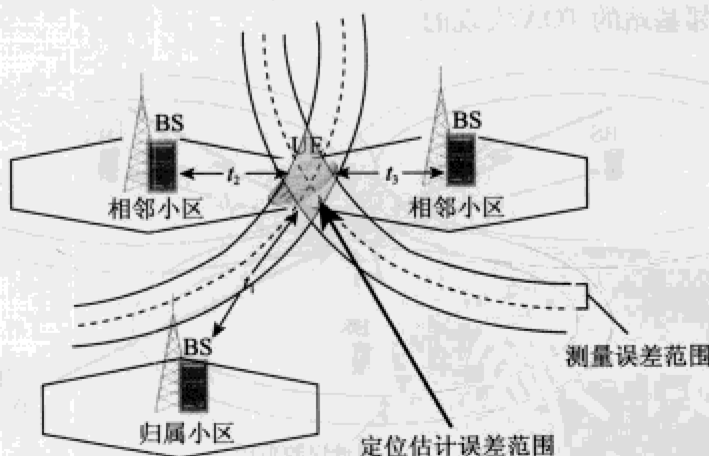


图 8.14 TDOA 定位

因此，TDOA 方法的基本思想是通过测量信号到达目标（终端或者基站）的时间差，而不是绝对到达时间来确定终端的相对位置。如果得到了相邻基站之间的时间差，并且终端和基站之间存在 LOS（视距路径），那么移动终端就位于双曲线上：

$$D_1 - D_3 = c\Delta t = c * GTD = \sqrt{(X_i - x_m)^2 + (Y_i - y_m)^2 + (Z_i - z_m)^2}$$

其中，D_i 是手机到相邻基站的距离，c 是光速，Δt 是来自相邻基站信号的到达时间差，X_i, Y_i 和 Z_i 是相邻基站的坐标，(x_m, y_m, z_m) 是移动终端的坐标。如图 8.14 所示，通过测量三个不同基站的两个 TDOA，就可以根据双曲线的交点估计出终端位置。不过，为了获得唯一且更精确的估计，应该与三个或更多个基站进行比较以获得至少三个时间

差测量。

8.3.4.1.4 E-OTD

E-OTD的基本原理和TDOA方法类似。与TDOA一样,E-OTD也是通过测量相邻基站的时间差来对移动位置进行估计。因此有时会认为该方法和TDOA方法是一样的。但E-OTD采用了更精确的测量步骤来提高定位精度。E-OTD所使用的测量方法称作“增强的OTD”。这里的OTD纯指测量的时间值,不要和E-OTD混淆,E-OTD是指定位方法本身。我们需要更准确的测量方法(尤其是当网络不同步时),这种方法同时适用于GSM系统和WCDMA(宽带码分多址)系统。

OTD测量在LMU(定位测量单元)和MS(移动台)两处进行。BSC或SMLC通过比较两组OTD测量值来决定定位估计。由于OTD测量报告会引起额外的信令,故此LMU的OTD测量结果只是按一定的时间间隔报告给SMLC。报告OTD结果的频率取决于BS可用的资源以及请求业务所要求的精度。

8.3.4.1.5 TOA定位

在TOA方法中,位置计算基于无线信号从移动设备到基站的传输延迟。如果至少有三个TOA测量值可用,就可以用三角知识估计出终端的位置,方法是最小化终端和相应的TOA圆周之间的最小平方距离。图8.15示出了估计终端位置的原理,它是通过测量三个相邻基站的TOA实现的。

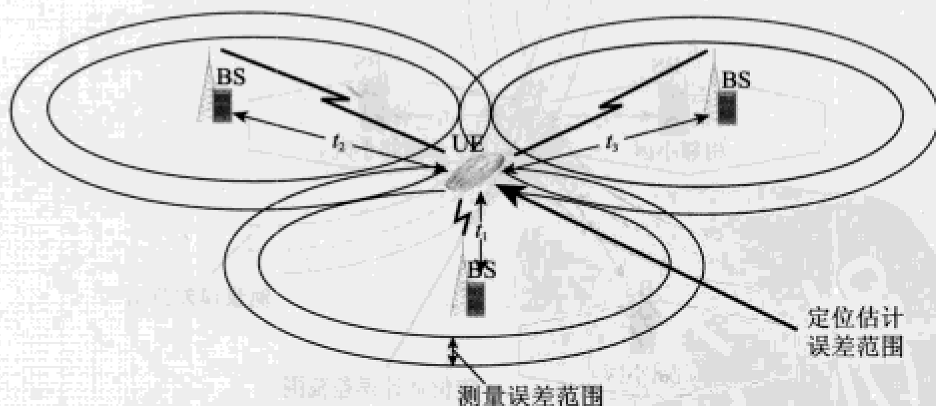


图8.15 TOA定位

在TOA方法中,终端到基站的距离正比于传输时间t_i。如果手机和基站之间有LOS,它们之间的距离为:

$$D_i = ct_i$$

其中c代表电磁波的速度,t_i代表信号从基站到终端或终端到基站的传输延迟时间。在实际当中,由于NLOS(非视距路径)、信号衰落、反射和阴影以及小区边缘覆盖变化等原因,TOA测量总有一定误差。因此在估计TOA定位精度时应当考虑到测量误差的范围。

从图8.15来看,为了获得唯一的移动终端位置估计,至少需要三个基站的TOA。

然后用最小二乘法计算终端和几个基站之间的距离，从而可估计出手机的位置。即：

$$D_i = \sqrt{(X_i - x_m)^2 + (Y_i - y_m)^2 + (Z_i - z_m)^2 + \varepsilon}$$

其中，(X_i, Y_i, Z_i)代表定位过程所涉及相邻基站的坐标，(x_m, y_m, z_m)代表待定位终端的坐标。

TOA 方法要求非常精确的基站同步，这对于不同步的蜂窝系统可能是一个挑战。位置计算实体也应能识别出发射和接收信号之间的时间差。TOA 方法最大的好处是不一定需要对移动设备进行升级，尽管网络的升级费用可能是一个问题，因为在移动网络中它被广泛接受。

8.3.4.1.6　AOA

终端的位置也可以通过两条代表导频信号分支的直线的交点来确定，每一条直线形成一个从基站到移动终端的夹角。每个测量的角度形成许多对直线从而能确定出目标手机的位置。如图 8.16 所示，如果移动终端和两个基站之间存在 LOS，两个相邻基站之间的 AOA 可以测得，那么移动终端的位置就是到达角度所确定的直线的交点。

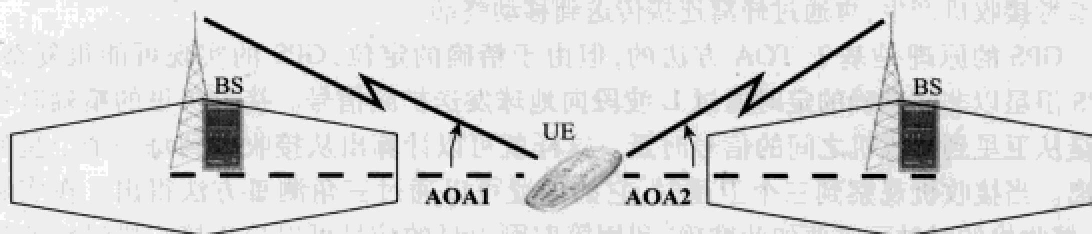


图 8.16　AOA

与 TOA 和 TDOA 方法相似，AOA 方法也可以通过超过两个以上的测量值来提高准确性。然而，反射和绕射会引起严重的误差，特别是在城市环境中使用 AOA。移动终端自身一般不能确定其 AOA，所以 AOA 应该在基站中测量。

AOA 对信号衰落很敏感，因此 AOA 和其他技术（比如频率复用）联合运用时需要更精细的网络设计，并且对网络容量规划的要求也较高。AOA 方法实现起来非常复杂和昂贵，因为在基站接收端需要几个大天线。但在另一方面，许多已有的基站可用于这一目的。

8.3.4.1.7　RNBP

RNBP 方法有时也叫作“本地定位”或“自定位”，其原理是选择一个参考节点来提供移动设备的辅助定位测量值。参考节点可以是移动的或者固定的，可以有中继或者重发功能。参考节点可以是定位服务设备、GPS 接收机或者其他位置已知并能作为终端定位参考点的设备。在有些环境下，可以利用短程无线电通信（如蓝牙、WLAN 或 UWB）把位置信息从另外一个邻近且位置已知的设备传送到移动终端。这样，移动终端通过测量来自参考节点的信号强度或传输时间就可以计算出自己的位置。由于使用短程无线通信的移动设备数量正快速上升，RNBP 的可行性和精度将大幅度提高。特别对于室内应用，预料 RNBP 将会成为普遍采用的方法。

除了基本的信号传输时间和信号强度以外，RNBP 至少在原则上可以结合其他定位方法，比如 TDOA、TOA 或者 AOA 等。要点在于，RNBP 通过利用网络中附加的参考设备可以提供增强的定位。RNBP 可以用来改善基于网络的定位方法，例如通过在 RAN 中加入所谓的"种子节点"。RNBP 方法有成本方面的缺点，因为 RNBP 必须放置于基站或者类似位置，而且每个 RNBP 也需要单独的天线。不过成本问题也许并不突出，因为现有无线网络结构已经具备放置节点和重发器的位置。但在任何情况下都需要进行仔细的网络规划以避免重发器引起的干扰增加。

8.3.4.1.8 GPS

GPS 是基于卫星的定位系统，在很多方面它是当前可用的最好的无线导航辅助。GPS 由美国政府来运作，用于军事和公众目的。

GPS 可以多种方式与蜂窝应用相结合。首先是在终端中安装一个 GPS 接收机，它和单独的 GPS 接收机一样。通过向终端发射 GPS 辅助数据，可以显著提高 GPS 接收机的准确性和速度。这使 GPS 在蜂窝网络中非常有用，因为 GPS 辅助数据可以由一些参考接收机产生，再通过蜂窝连接传送到移动终端。

GPS 的原理是基于 TOA 方法的，但由于精确的定位，GPS 的实现可能很复杂。GPS 卫星以非常精确的定时通过 L 波段向地球发送扩频信号。接收机里的精确时钟测量从卫星到接收机之间的信号时延。这样就可以计算出从接收机到每一个卫星的距离。当接收机观察到三个卫星时，它的位置可以通过三角测量方法得出。在实际中，接收机的时钟不需要如此准确，利用第四颗卫星的信号可以校正接收机时钟的误差。来自 GPS 卫星的无线信号可以看作是围绕卫星形成了一个球体，可根据信号的传播时间画出。三颗卫星形成三个球，接收机的位置就是这三个球的交点，从而得到纬度、经度和海拔高度的坐标。图 8.17 示出了基于 GPS 的位置估计。

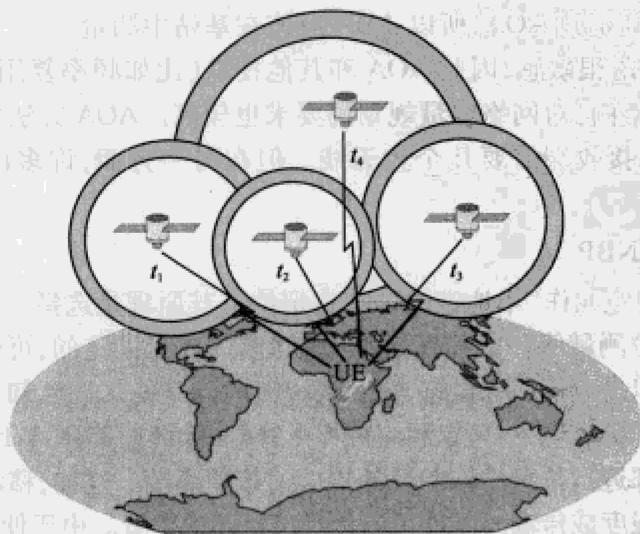


图 8.17 GPS 定位

GPS 定位是目前存在的最精确的定位系统之一,尤其在 DGPS(Differential GPS,差分 GPS)辅助下。不过 GPS 接收机一般要求对四颗卫星有 LOS,这是一个问题,特别在室内。另外,GPS 接收机有一根专用的卫星天线,它通常相对很大,可能会干扰蜂窝的使用。GPS 接收机增加了移动终端的制造成本和功率消耗。为了克服或者至少缓解这些问题,GMS 和 UMTS 中的 GPS 定位和 GPS 辅助数据传送已经标准化。

8.3.4.1.9 Galileo 卫星导航系统

Galileo 是由欧盟和欧洲航天局联合发起的。

Galileo 星座包括 30 颗卫星,轨道高度约 24 000km,计划在 2008 年开始运行。它将兼容 GPS 并且可以与之相互操作。这样就可以改善对导航卫星的接入,并能改进定位精度和响应时间。Galileo 计划比 GPS 提供更高的精度。

Galileo 的工作原理和 GPS 类似:卫星装备有非常精确的时钟,卫星发送的信号能指示这个精确的时间。移动终端从几个卫星接收信号并测量信号的到达时间。利用这个测量结果及显示的时间,移动终端就可以根据与测量卫星的距离来计算出自己的位置。关于 Galileo 的更多信息可以登录网站:http://europa.eu.int/comm/dgs/energy_transport/galileo/index_en.htm.

8.3.4.2 定位精度

如前所述,除了基于小区信息的方法以外,各种定位方法的主要原理都建立在无线信号的传播特性之上,而无线传播特性不容易预测。蜂窝定位方法的准确性取决于蜂窝环境、无线连接的质量(例如接近 LOS 的程序)、信号测量值、接收机特性和计算方法。

基于小区 ID 方式的精度主要取决于无线网络中小区的结构和大小。对于有宏小区的网络,定位精度在几公里到几十公里范围内。在微微小区和微小区环境中,精度在几十米到几百米范围内。

TOA 方法的精度取决于信号衰落、阴影以及可以对多少个基站进行信号测量。要得到准确的移动终端定位估计,必须要有若干个基站存在 LOS。然而这样的要求和蜂窝网络一般的规划原则是相抵触的,所以蜂窝网中并不是任何地方都能达到这种方法的最优精度。

和 TOA 方法一样,TDOA 方法的准确性也受蜂窝网络环境、无线信号的固有特性以及可获得的测量值数目的限制,尤其对于非视距情形。不过 TDOA 只测量时间差,当采用 TDOA 时有些对所有基站相同的误差在定位过程中可以削除,所以在相同条件下基于 TDOA 方法的精度通常要比基于 TOA 的方法好。

总而言之,没有一种绝对合理的办法可以概括不同定位方式的准确性。不过我们对不同定位方法的精度还是有一个大体的判断,如图 8.18 所示。越精确的方法成本越高。性价比最好的方法是选择对某个特定的应用足够精确的方法。不同类型的 LCS 有不同的精度要求,所以同一网络中可同时使用多种方法。

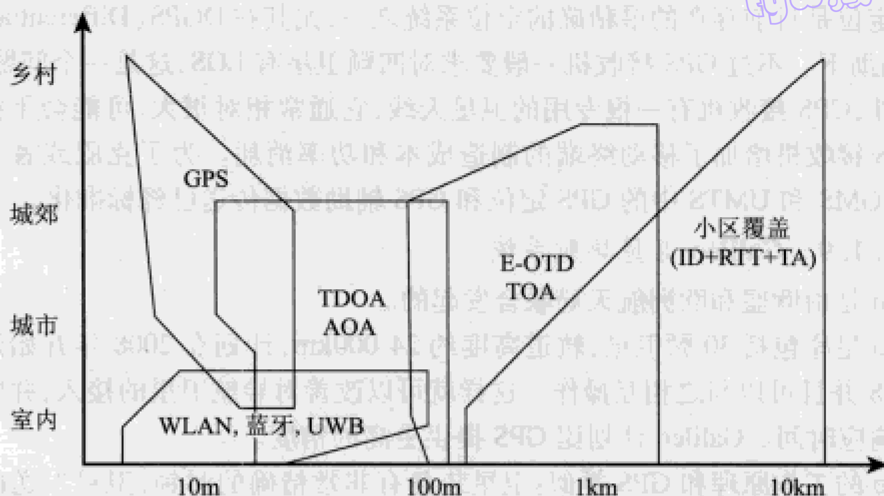


图 8.18　不同定位系统的精度比较

8.3.4.3　UMTS 和 GSM 规定的定位方式

3GPP 从标准化的角度对上述所有定位方法进行了研究和讨论。最终选择了三种用于 UMTS RTRAN 网络的定位方法。

- 基于小区 ID 的定位，小区 ID 在 UMTS 中对应 SAI（Service Area ID，服务区 ID）。
- OTDOA（观察的到达时间差）定位，顾名思义，它是基于前述的 TDOA 原理的。
- GPS 辅助定位。

对于 GERAN 网络，3GPP 标准选择了下列方法。

- 基于小区 ID 的定位。
- E-OTD（增强的观察时间差定位）。
- GPS 辅助定位。

这些方法原则上可以是基于网络的、基于移动终端的、基于网络且移动终端辅助的，或者基于移动终端且网络辅助的。它们之间的区别在于位置的计算在网络中进行还是在终端中进行，再就是产生辅助数据的位置，所以有网络辅助或是移动终端辅助的说法。下面几小节将深入介绍 UMTS 和 GSM 规定的定位方式。

8.3.4.3.1　UMTS 和 GSM 中基于小区 ID 的定位

在基于小区 ID 的方法中，SRNC（服务 RNC）把小区 ID 映射到相应的 SAI。如果 UE 处于小区不明确的情形，如处于软切换状态或者处于 RRC（无线资源控制）状态时，还需要基他的操作。在 GERAN 网络中，小区 ID 由 BSC 处理并在 LCS 中使用。

在软切换状态下，UE 有连接到不同小区的不同信号分支，从而报告不同的小区 ID。此时综合所有 SRNC 中可用的信息可以改善基于小区覆盖的定位精度。

小区 ID 的选择一般是基于接收信号分支的质量参数。也就是说，SRNC 选择信号分支最强的小区 ID 作为 UE 位置估计时的参考。也可以选择在连接建立中产生的第

一个小区 ID 作为位置估计的小区。除了这些普通的机制外，还规定了其他一些准则来确定切换时的小区 ID。

小区 ID 可以根据终端接收到的激活的基站集中的主公共导频信道（WCDMA-FDD 中的 CPICH）来确定。另外，激活集外的 CPICH 也有可能变得比主要的激活集中的 CPICH 要更好，此时可用排除的 CPICH 来确定到底用哪个小区 ID。

基于小区 ID 的方法应在 RRC 的各种连接状态下都能支持 UE 定位，如 URA PCH、小区 PCH、小区 DCH、小区 FACH、小区重选、系统间模式和空闲模式等。

如果 UE 不处于激活状态（例如，UE 至少和其中一个小区之间没有连接），就不可能获得小区 ID。例如在 UMTS 中，仅当 UE 至少和一个 BS 之间存在 RRC 连接时，才能提供小区 ID。因此，若 UE 处于空闲状态，就迫使其进入一个能提供小区识别号的状态。例如在 URA PCH 状态可能没有小区 ID，于是 UE 被强制转换到具有小区 ID 的状态（如小区 FACH 状态）来确定小区识别号。当 UE 选择新的小区时，为了接收小区 ID 的更新，网络也可以阻止 UE 进入 URA 更新状态。当 UE 处于空闲模式或者 URA PCH 模式时，为了定位，需要通过 CN 或者 UTRAN 对其进行寻呼。如图 8.19 所示。

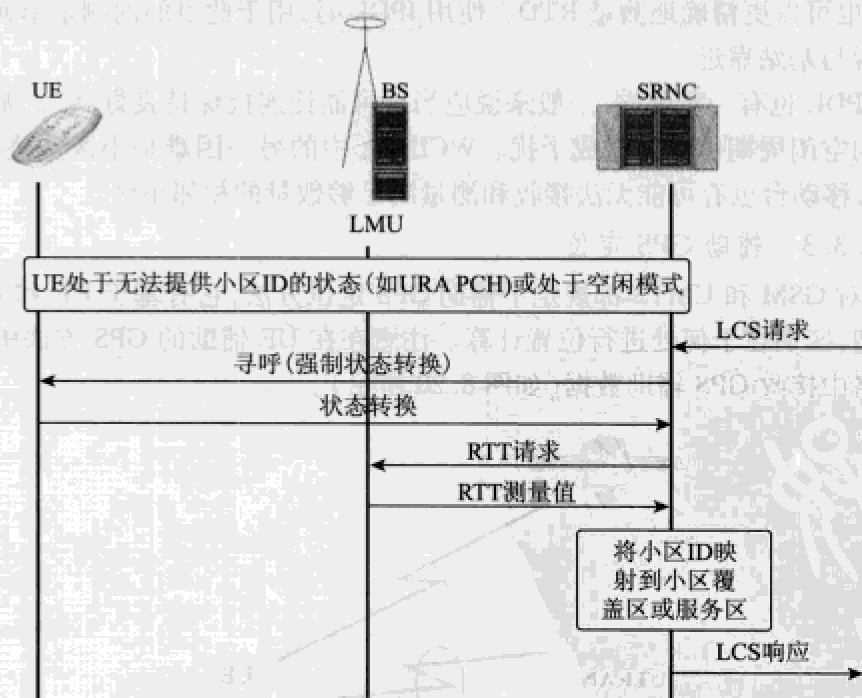


图 8.19 基于小区覆盖定位的一般过程

在 UTMS 中，UTRAN 因素应该对 CN 隐藏。因此需要把小区识别码映射到 SAI，SAI 通过 Iu 接口从 UTRAN 发送到 CN。服务区原则上可以包含多个小区，但目前 UTRAN 中的小区 ID 和 SAI 是一一对应的。

8.3.4.3.2 UMTS 中的 OTDOA-IPDL

UMTS 中的第二种定位方法是 OTDOA-IPDL（下行链路空闲周期观测到达时间

差)方法,它由两部分组成。首先是OTDOA,在理论上和先前所描述的TDOA相似,不过为了估计UE的位置,OTDOA更着重于UE测量相邻基站之间的观察时间差。

在WCDMA-FDD中,测量OTDOA和RTD不是很直接,有以下两个原因。

- 有时可能没有足够的下行导频信号用于UE测量。例如UE离服务基站非常近的时候,基站强信号的发射将阻塞其接收机。这个问题也称为"可听效应"。
- WCDMA-FDD中基站通常是不同步的,在计算终端位置之前,必须先知道或者测量基站间的同步差RTD。

为了解决这些问题研究了两个可能的解决方案来支持WCDMA-FDD网络中的UE定位,先是在日本标准实体中,后来在3GPP中。

第一个解决方案是临时提高邻基站的发射功率以使UE能测量它们。但是,WCDMA-FDD和所有基于CDMA的无线技术一样是干扰受限的,这个增加功率的方法会显著增加网络中的干扰,因此是不可行的。

另一个解决方案是让服务基站在短时期内停止发射以缓解可听性问题。这种方法称为IPDL(下行链路空闲周期)。在服务基站的空闲周期,UE可以测量相邻基站的信号,同时也可以更精确地测量RTD。使用IPDL时,用于此目的的测量单元可以置于基站中或者与基站靠近。

使用IPDL也有一些弊端,一般来说应当尽可能让连接保持良好状态,基站发射中这种定期的空闲周期可能会造成干扰。WCDMA中的另一困难是小区重叠很少,即便用了IPDL,移动台也有可能无法接收和测量出足够数量的相邻小区。

8.3.4.3.3 辅助GPS定位

3GPP对GSM和UMTS都规定了辅助GPS定位方法,它有基于UE和UE辅助这样两种类型,区别在于何处进行位置计算。注意在在UE辅助的GPS方法中,UE也有可能从网络中接收GPS辅助数据(如图8.20所示)。

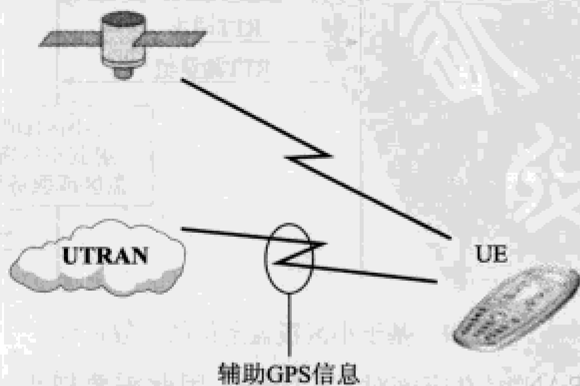


图8.20 UMTS系统中辅助GPS的基本原理

在基于UE的GPS辅助方案中,UE包括一个完整的GPS接收机,位置计算也在UE中进行。网络发给UE的GPS辅助数据包括以下两项。

- 测量的辅助数据，即 GPS 参考时间、可视的卫星列表、卫星信号的多普勒和码相位搜索窗口。这些数据在 2~4 小时内有效。
- 用于位置计算的辅助数据，即参考时间、参考位置、卫星星历和时钟校正。这些数据在 4 小时内有效。

采用差分 GPS 时，差分校正数据也将发送到终端。这种辅助数据大约在 30s 内有效，但与一个很大的地理区域相关，因此可以只用一个位于中心的参考接收机来产生辅助数据。

在基于网络且 UE 辅助的 GPS 方案中，UE 只有一个简化的 GSP 接收机，用于伪距测量并把测量结果发送到网络中的计算单元，该单元完成其余的 GSP 操作。这个方案中网络只向 UE 发送少量的辅助数据，但 UE 要在上行方向发送所有的测量结果。和基于 UE 的模式相比，UE 辅助的模式中参考时间必须更为精确。

8.3.4.4 LCS 的系统结构

UMTS 中的 LCS（定位业务）功能分布于现有网元中，基本上和 GSM 一样。为了支持 LCS，GSM 和 UMTS 都在整体系统结构中增加了一个主要的新网元，即 GMLC（Gateway Mobile Location Centre，网关移动定位中心）。

图 8.21 示出了 UMTS 中 LCS 的整体结构。LCS 设备和功能同时位于 CN 和 UTRAN 中。UTRAN 实体用上述方法测量和收集定位数据并确定移动设备的位置。在 CN 中 GMLC 作为一个连接点，定位数据通过这个连接点传送到其他业务功能或者客户应用中。

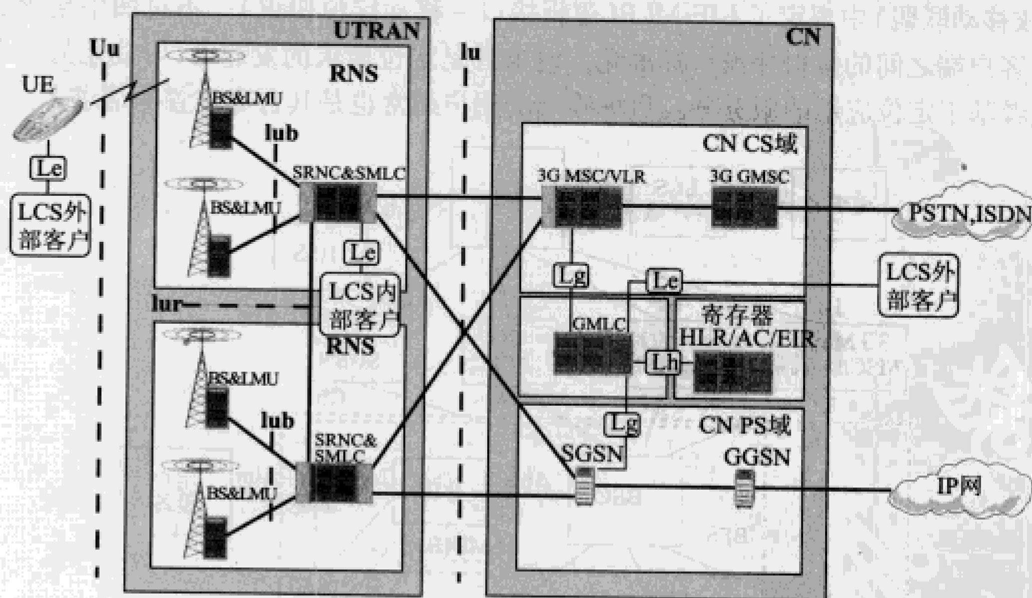


图 8.21 UMTS 中的一般 LCS 结构

UMTS LCS 系统结构和 GSM 中的 LCS 结构很类似，但是在 UMTS LCS 中，为了降低复杂性省去了一些可选的网络方案。与 GSM 相比，基于 WCDMA-FDD 的 UT-

RAN在蜂窝定位方面既有限制，也有优点。

在UMTS中，SRNC在控制无线接入中起关键作用，包括无线资源管理。包括软切换测量在内的无线链路测量都是由SRNC终止和控制的。由于30%～40%的呼叫都涉及软切换，因此很多时候SRNC可以得到这些可用于定位的测量结果。因此在考虑UMTS中LCS的结构时，可以合理地利用WCDMA-FDD的这一优点。其结果是，对应于GSM中SMLC的功能在UMTS中分配给了SRNC。

不过对于辅助GPS来说，定义了一个独立的SMLC，它可用于基于移动台的GPS和移动台辅助的GPS。

和GSM中的许多可选方案相比，在SRNC中包含了主要的SMLC功能这一方案简化了Iu、Iur和Uu接口的信令规范。UMTS的主导原则是把无线相关的方面和CN分开，LCS也如此。

GSM中的SMLC可以是专用的物理网元，也可以集成在BSC中。在LCS标准化的早期，SMLC既可以放置在接入网中也可以放置在CN中。

GSM中的SMLC和UTRAN中的SRNC选择定位方法、控制定位测量并计算目标终端的位置，计算所用的测量结果来自目标终端本身或者专门的LMU，LMU位于基站中或者连接到基站。

3GPP的LCS规范以更为正式的方式给出了不同网元中的LCS功能及其网元间的相应接口。图8.22是GERAN中的3GPP LCS参考模型，图8.23是UTRAN中的LCS参考模型。图中的接口和网络实体在相应的3GPP LCS标准中都有规定，在OMA（开放移动联盟）中规定了LIF-MLP（逻辑接口－移动定位协议）。不过图中请求者和LCS客户端之间的接口并没有标准化。请求者是定位请求的发起者，可能是另一个终端或者基于定位应用的服务器。目标终端的用户通常也是其自身位置的请求者。

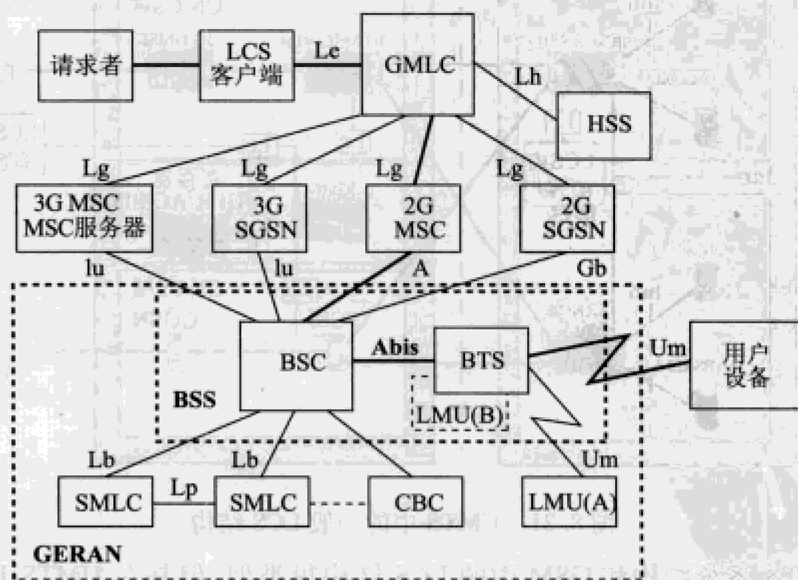


图8.22　GERAN中的LCS参考模型

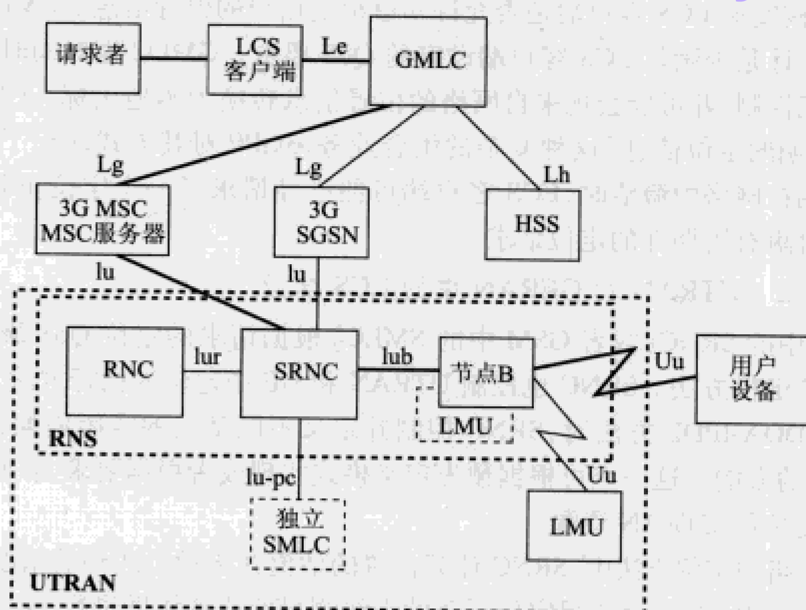


图 8.23 UTRAN 中的 LCS 参考模型

8.3.4.4.1 CN 中的 LCS 功能

CN 中的 LCS 功能体分布在 MSC/VLR、MSC 服务器、SGSN、HLR/HSS 和 GMLC 上。MSC/VLR 和 SGSN 可以发起 LCS 目的的寻呼，处理 UE 鉴权以及呼叫相关或呼叫不相关的定位请求和计费。

用户可以控制是否对不同的 LCS 客户公开其终端位置以及怎样公开。这一点由 LCS 私有类在用户配置中定义，它保存在 HLR 或者 HSS 中。对于 VASC 增值业务，用户希望每次他的位置被请求时可以给出提示，然后由用户决定接收或者拒绝来自指示 LCS 客户端的位置请求。网络将把这种私有调用请求只发送给那些能够处理这种请求并能显示给用户的终端。终端通过“UE 类别标志”告诉网络它在这方面的能力。UE 发送类别标志 2（即 CN 类别标志）到 MSC/SGSN 以表明 UE 是否支持私有验证。

UE 也发送类别标志 3（即 RAN 类别标志）至 RNC（在 GSM 中发送到 BSC 和 MSC）表明所支持的 LCS 方式。CN 不需要这个信息。

GMLC、MSC 和 SGSN 处理所有涉及 LCS 的费用和账单问题，包括客户端和用户的费用和账单，后者包括本地用户以及来自其他 PLMN 的漫游用户的费用和账单。MSC 和 SGSN 也授权为特定的 UE 提供定位业务，其方式如同其他蜂窝业务。MSC/VLR 处理 CN CS 域中的 LCS，SGSN 支持 CN PS 域中的 LCS。

HLR 包括用户数据以及使用 LCS 时的私有配置，也包括移动终端当前所注册的 VLR 或 SGSN 信息。GMLC 用 MAP 信令通过 Lh 接口从 HLR 请求路由信息，即移动终端当前注册在哪个 VLR 或 SGSN。

GMLC 用作外部 LCS 客户端和移动网络间的网关，并把 LCS 客户端的定位请求转发到 HLR 所指示的 MSC/VLR 或者 SGSN 中。GMLC 在 HLR 的协助下对 LCS 客户

进行签权，即核实该LCS客户端是否允许知道给定用户的位置信息。CMLC判断来自网络的位置估计是否满足LCS客户端设定的QoS要求。GMLC也对同时或同期的定位请求提供流控制，并可能会把来自网络的位置信息转换为本地坐标。CMLC应该处理“延迟和周期的定位信息”这种复杂的组合业务，3GPP对其方式作出了规定。当给定的移动终端在网络中激活时，LCS客户端可能已经请求了一个定位报告，对同一用户并可能同时附有周期性的定位请求。

8.3.4.4.2　UTRAN和GERAN中的LCS功能

UTRAN中的SRNC(或者GSM中的SMLC)根据请求的定位QoS级别选择可能满足此要求的定位方法。SRNC也控制UTRAN和UE中定位的执行方法。

采用OTDOA-IPDL方法时，SRNC控制并定义不同基站的空闲周期，以最小化对UTRAN性能的影响。这一点可根据预先定义模式实现或者根据要求实现。RNC也协调涉及终端定位的UTRAN资源。

在基于网络的定位方法中，SRNC计算位置的估值并指示可达到的精度。它也控制基站中的大量LMU，目的是获得定位需要的无线测量值或者协助进行UE定住。SRNC和LMU之间的信令通过Iub接口传输，在有些软切换情形中也可以通过Iur接口传输。

在UMTS中，LMU一般集成在BS中，可能不会规定单独的LMU。LMU的主要功能是测量不同基站的RTD、参考时钟的ATD(Absolute Time Differences，绝对时间差)，或其他各种基站发送信号的无线接口定时测量值。LMU返回给SRNC的有些测量结果可用于多种定位方法。LMU获得的所有位置测量值和辅助测量值只发送给和对应基站相关联的SRNC。SRNC以直接或预定义的方式控制基站中的定时和任意LMU测量值的周期。

8.3.4.4.3　UE中的LCS功能

依定位方式的不同，UE将以不同的方式涉及定位过程。例如在基于网络的定位中，UE不计算它的位置，而在基于移动终端的定位中计算。UE也可以装配GPS接收机来独立定位。GPS移动终端可以向网络请求GPS辅助数据以加速定位过程、提高精度或GPS接收机的灵敏度。在基于网络的辅助GPS方法中，有GPS接收机的UE的定位在网络中决定，GPS测量结果由UE报告。

移动终端可以请求网络来确定它的位置(网络辅助定位)，移动终端也可以利用自己的测量结果和网络的辅助数据确定自己的位置。

使用IPDL要求UE能够测量和存储空闲周期中的无线信号定时，并能把不同的BCH(广播信道)码与不同的空闲周期模式关联起来。UE需要确定服务基站和其他基站的第一个可检测路径的到达时间。然后UE把测量结果报告给SRNC或SMLC。

8.3.4.4.4　LCS客户端和GMLC

LCS客户端可能驻留在某个服务器中，该服务器利用移动终端的位置信息提供业务和应用。LCS客户端通过GMLC向PLMN(蜂窝网络)请求一个或多个目标终端的位置信息。这个请求包括了一组参数以定义请求的精度、响应时间及其他事项。

UMTS 的主要接口(即 Uu、Iub、Iur 和 Iu)大都支持 LCS。除此还为 GMLC 定义了特定的 LCS 接口,如图 8.22 和图 8.23 所示。

- LCS 客户端和 GMLC 之间的接口称为“Le”。LCS 客户端通过这个接口发送 LCS 请求,GMLC 把相应的结果返回到 LCS 客户端。
- Lh 是 GMLC 和 HLR(HSS)之间的接口。GMLC 利用这个接口从 HLR 获得 CS 和 PS 域的路由信息。
- GMLC 通过 Lg 接口连接到 MSC/VLR 或 SGSN。对指示目标终端的位置请求通过 Lg 接口从 GMLC 发送到当前服务该 UE 的 MSC/VLR 或 SGSN,MSC/VLR 和 SGSN 则向 GMLC 返回定位结果。

Lh 和 Lg 接口都是基于 MAP 协议的。

8.3.4.5 用户平面中的位置信息

上述的 LCS 功能都发生在所谓的蜂窝网络的“控制平面”中,这意味着确定终端位置涉及多个网络节点,这些网络节点之间有标准化的信令。所有涉及的网络单元都必须能够互相通信,于是可能出现的一种情形就是网络的定位能力会受到系统中最不先进的网络节点性能的限制。在网络中还存在相互兼容的问题,因为设备来自不同的厂家,或者网络中的设备分属不同的代,有些需要更新才能实现 LCS 的全部功能。

克服以上这些弊端的一种方法是在网络中建立终端和服务器之间的 PS 数据连接。该连接可以由服务器或终端来请求,蜂窝网络按普通数据连接一样建立连接。数据连接携带用户数据,因此说它是在“用户平面”中。利用这种数据连接,服务器可以传输 GPS 辅助数据给终端,终端应用也可以向服务器传送位置信息。

用户平面位置方案在 OMA 和 3GPP2 中被规范化,其目的是达到与控制平面方案相类似的功能。用户平面方案也需要符合常规的隐私要求,并能支持 GPS 辅助数据的计费。由于位置信息在紧急情况下的重要性,根据常规要求,一些国家规定用户平面方案也必须支持紧急呼叫。

8.3.4.6 LCS 中的用户隐私

从隐私角度说,位置信息属于敏感信息,人们可能不愿意让任何人随时知道自己的位置信息。在如何处理位置信息方面也有严格的规定,如不允许存储用户位置信息。标准化机构已经意识到了隐私的重要性并已经制定了若干机制来加强位置信息方面的隐私规则。根据 3GPP 标准,目标移动用户可以根据不同的情况制定处理位置信息的规则。隐私规则可应用于特定的 LCS 客户端或已知的请求方。在用户未对 LCS 客户定义任何隐私规则时,默认处理是不允许定位。用户也会希望能对呼入的定位请求给出通知,并能有机会拒绝或接受这一请求。此外,用户可以设置一个密码,供朋友或信任的应用使用。当定义有密码时,只有当请求者或应用能提供正确密码时才能得到位置信息。对于导航类的定位业务,只有精确的位置信息才是可用的,而其他如提供本地信息之类的业务不需要这样精确。根据标准,用户可以据此设备“业务类型”隐私规则,该规则只允许某些业务类型得到位置信息,但阻止其他业务获得位置信息。

8.3.4.7 使用位置信息的业务实例

在蜂窝网络中,位置信息和基于位置信息的业务经常作为高级业务的例子提及。移动电话用户可以自由走动,可以自由地在任何地方发出或接收呼叫,或启动业务。很明显,位置信息可以使这些业务更强。还有一些服务专门针对有位置信息的情形。本节介绍利用位置信息优点的一些业务,现在从最明显的导航开始介绍。

8.3.4.7.1 导航

某些情况下导航业务对多数移动用户来说是相当有用的。当你进入一个城镇,或者在一个陌生的地方下车时,你可能很希望有那里的地图。你可能想要找一个具体的地方,但不知道这个地方和你现在的位置是什么关系(如图8.24所示)。另一个很明显的需求是找出到达某个地点的最短路张。LCS 可以直接用在这些情况中。首先,导航业务需要确定出你目前的位置,其次你需要给出你的目标地址(即你要找的地方)。这看上去可能很简单,但要想使导航业务良好地工作,需要解决几个难点。首先,你和业务提供商之间需要对位置的描述方式协商一致,比如用建筑名、街道地址或地理坐标。由于坐标有明确的定义,因而对于导航是最理想的方式。不过人们通常都不用坐标来说一个位置,所以需要将坐标转换成建筑名或街道地址。建筑名或地址可以表示为地图网格中的一个方格,如图8.24所示。导航服务一般和话机中显示的电子地图一起使用。指路的功能也可以是文本消息或语音,即便如此,地图也是一个有用的备份。

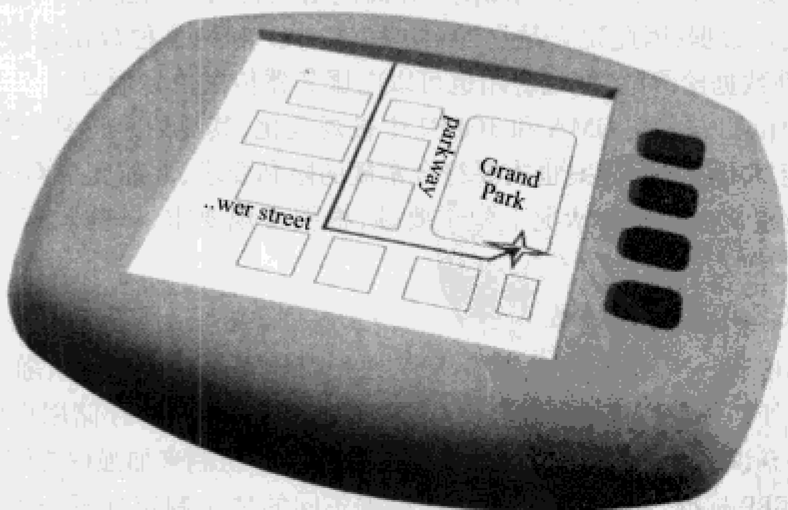


图8.24 LCS 业务中"指路"的例子

8.3.4.7.2 找出邻近的东西

上面的例子说明了在到达一个城市时获得本地信息方面的用处。当用户进入一个给定的位置时,可以把与位置相关的信息发送给用户的终端设备,也可以是用户根据需要来请求位置信息。此类业务非常接近市场,可以免费或以很低的价格向用户提供。另一方面,用户可能也愿意为有价值的信息付费,因此对这类服务可能需要建立

成本和收益的平衡。提供的信息必须要保持更新,因为这方面的竞争对手仍是电话簿和黄页,而且电话簿和黄页往往可以在线查询。

8.3.4.7.3 运输管理

运输管理明显要用到位置信息,这样的信息可以提高运输的效率,从而使成本更低。如果能知道车队中每辆车的实时位置信息,就更容易计划并有可能对一些运输进行合并。根据交通条件和运输计划等的变化,运输控制中心可以优化工作计划并通知司机。位置信息可用于跟踪运输的包裹,检查其进度。可以做到实时跟踪,但这样做成本太高,一般没有必要。运输过程中的定位信息精度可以从几千米到几米不等。在跟踪被盗车辆和紧急情况等情形下,提供精确的位置信息非常重要。

运输相关的服务还有出租车的分派、导航和监视。控制中心可根据出租车的位置信息分配一辆最近的车给顾客。这对顾客来说是节约了等待时间,对车队来说是提高了效率。可以向客户告知出租车大概多长时间能到,出租车司机也可以利用前述的定位系统导航。

8.3.4.7.4 游戏

网络游戏令很多人着迷,那些对游戏上瘾的人花费了大量时间玩游戏。很多网络游戏需要充分利用配置很高的个人计算机的图形和计算能力,其他一些游戏创意紧凑,玩起来比较简单。移动设备明显不具备 PC 机的处理能力,但从另一方面说它们有移动的能力。如果手机也是游戏机,就会有用户为了玩游戏而一直在线,由于手机在随着用户移动,就有可能把游戏和手机的位置信息结合起来。

这样的游戏有很多,比如寻宝,玩家收到一个文本消息,告诉他一个新的宝藏在某个位置,先到(足够接近即可)的人得到这个宝藏。没有被发现的时间越久,宝藏的价值也越高。另一个游戏是"捉迷藏":用手机找到其他用手机的人及其位置。

8.3.4.7.5 网络优化

除了针对终端用户的基于位置的业务以外,位置辅助数据也可以用于网络规划、无线资源管理机制、移动性管理机制、网络维护和性能管理等方面,从而可以优化系统的性能。这就使网络设计者和运营者可以根据移动设备的位置信息对其网络进行优化。在规划网络时,用户的基本信息对于制定网络规模、开发计费策略、网络自动管理(如结合掉话、阻塞与故障排版)十分重要。位置信息也可以作为输入来控制 BS 的发射功率和波束成形机制,以根据移动设备的情况提供自适应的覆盖。这一类的应用不需要很高精度的位置信息,可以重复使用其他服务所提取的位置信息。

切换控制就是利用位置信息优化网络相关特征的典型例子。假设移动台处在一个微小区中,还有一个宏小区重叠在微小区簇上(如图 8.25 所示)。假如一个快速移动的移动用户正在穿越微小区,那么快速移动的用户就必须得频繁重选微小区,给网络带来不期望的信令负荷。根据位置信息,我们可以预测其行为,于是可以把快速移动的用户切换到宏小区,从而减少额外的信令负荷。相反,可以把慢速移动的用户从宏小区切换到微小区以降低其功耗及其产生的干扰。

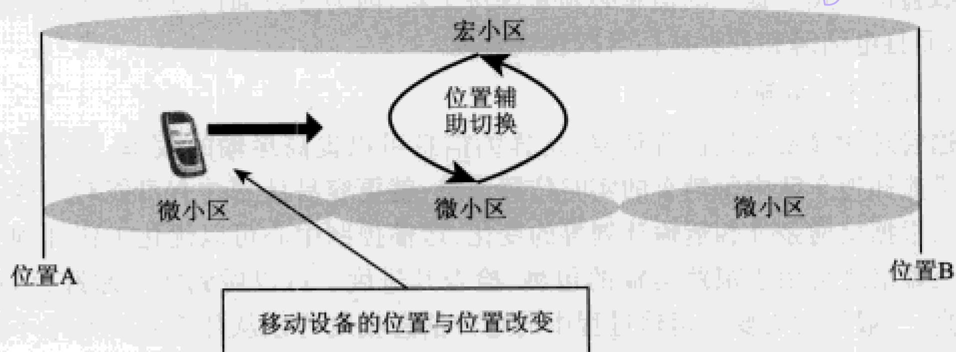


图 8.25　定位辅助的切换示例

位置信息使运营商有机会对其网络和网络管理系统进行优化。当与网络控制功能联合使用时，基于位置信息的测量值带给网络优化的价值还将显著提高，并能提高无线网络的智能性。这方面最大的困难在于用户隐私，这些应用要想可行就必须要先解决这个问题。

8.3.5　IMS 业务机制——短信

目前，网络可以提供各种形式的短信业务。简单地说，信息发送仅仅是把信息从一个实体发往另一个实体的方法，短信不仅可以有许多形式，而且还可以包含多种媒体形式，甚至还可以有多种发送方式。另外，IMS（见 6.5 节）还包括专门的短信服务功能。

IMS 短信业务有三种形式。

- 即时短信业务。
- 基于会话的短信业务。
- 延迟传送的短信业务。

每个 IMS 短信业务类型各有特点，使其实际上就像单独的业务（如图 8.26 所示）。不过就终端用户来看，它们都没什么差别，因为差别主要在技术方面，并且差别出现在网络内部。所有的这些 IMS 短信类型直接利用了 SIP（会话初始化协议）和 IMS 结构。

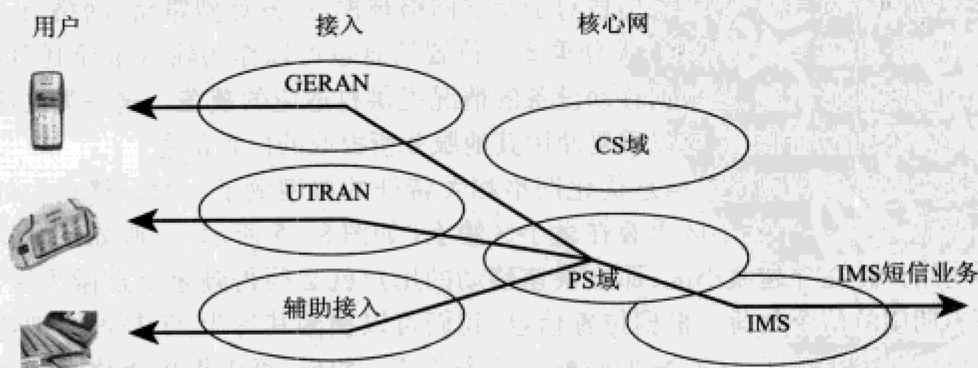


图 8.26　3GPP R5 中 IMS 短信业务的连接

在即时短信业务中，发送者使用 SIP 的消息方式给接收者发送信息（如图 8.27 所示）。这个方法用在“寻呼模式”中，涉及的通信只是发送信息和接收响应。这一业务的本质是随机的，就是说，它不是一个由很多信息对组成的会话。发送的短信可以只是纯文本，但也可以包含声音、图像等其他媒体类型。

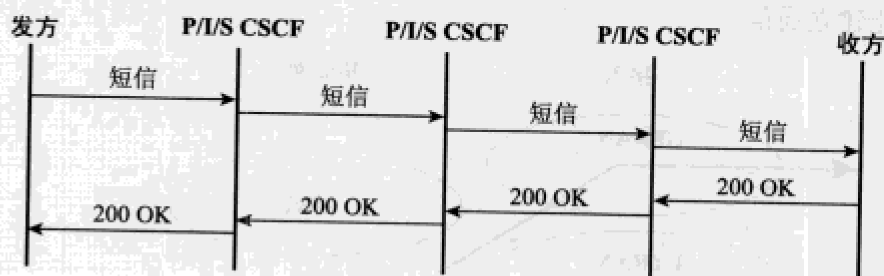


图 8.27 即时短信流示例

基于会话的短信业务已经用在传统的因特网中，被称为 IRC（因特网中继聊天）。在这种信息类型中，业务在相关方之间，每一方通过邀请过程加入会话。在 IRC 中，会话中交换的信息是文本信息，而 IMS 要在基于会话的短信业务中引入其他媒体成分，以达到丰富内容的目的。这将为新业务提供很吸引人的可能性。例如，能同时通过文本信道提供并行内容的视频呼叫对有听力障碍的人来说是很有意义的业务。

如果从终端用户的角度来看的话，延迟传输的短信业务已经有了：就是 MMS（多媒体短信业务）。在 IMS 中实现延迟传输的短信业务需要修改一些标准和定义，3GPP R6 版本处理了这一问题。

8.3.6 IMS 业务机制——呈现业务

我们将简要介绍的另一个与 IMS 相关的业务机制是“呈现业务”。呈现的意思基本有两点：它可以把一个人的状态提供给其他（特定的）人，也可以把另一方的状态提供给给定的请求者。

呈现信息包括下列几项。

- 个人可用性。
- 终端可用性。
- 通信偏好。
- 终端功能。
- 当前活动状态。
- 位置。

一个呈现业务并不一定会给出所有这些信息，每个用户都可以更改其呈现信息。

传统因特网中已经有这类业务。有些业务提供商提供了应用下载，可对特定的、所选的、提前定义的人物列表提供部分呈现信息。在因特网中，呈现业务用于消息方式，如让用户可以检查目标接收者是否在线。

如图 8.28 所示，在移动领域内范围就更广了。除了纯消息外，呈现业务还可以提供关于其他业务可能性的信息，如接收语音呼叫的能力、能否进行游戏等。这样，移动呈现应用就是因特网中呈现应用的扩展版本。呈现业务使用的一个可能发展就是动态电话簿，它包括关于电话簿入口的嵌入式呈现信息。有了这个信息，主叫方马上就知道能不能建立通信。



图 8.28　3GPP R5 中的 IMS 呈现连接

当然了，在呈现相关的业务中，安全是一个重要的关注领域。在任何情况下，任何人的呈现信息都不能让所有人可见。不过有些机制可以允许这么做。

- 公布呈现信息。呈现信息在呈现配置中，呈现配置的拥有人称为"呈现者"。呈现者定义他将怎样公布其呈现信息，谁可以看到，以什么级别看到。
- 观察呈现信息。若一个用户请求另一个用户已经公布了的呈现信息，他就是"观察者"。观察者只可以看到允许他看到的内容，可看的范围总由被请求的目标终端/用户定义。
- 定制呈现信息是一个 SIP 消息流，观察者通过这个消息流请求呈现信息。

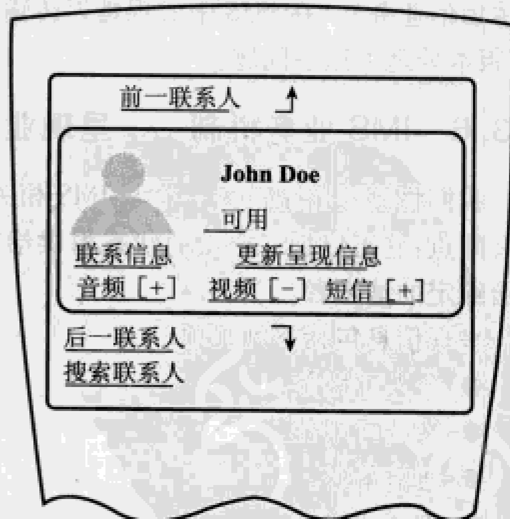


图 8.29　动态电话簿中的入口

基于呈现业务的一个自然应用就是"动态电话簿"（如图 8.29 所示）。对于用户添加到终端设备电话簿中的每个联系人，这种应用能显示该联系人的呈现配置信息。它对现有电话簿中的增值是：动态电话簿能使用户知道是否可以联系到期望的联系人，如果可以联系，联系人能接收什么样的媒体成分。

8.4 总结

本章简述了 UMTS 环境下一些与业务相关的内容。

如前所述，在 UMTS 环境中几乎可以创建任何业务，但仍然存在一些基本的问题，它们是用户真正需要的是什么？业务应向什么方向发展？这些问题的答案对电信业来说是至关重要的，这些答案的不确定性以不利的方式影响着移动通信行业。

在系统设计原则和业务区分方面，3GPP R5 以及进行中的解决方案为业务的建立和实现提供了新的、有效的办法。这些变化对终端用户来说并不是所有情况下都可见的，但新的实现方法使运营商有了更多的工具和选择。所有的这些新方法的最终结果很可能会提高整个业界的效率。

第 9 章
UMTS 环境中的安全问题

无线通信的特点是容易接入,不仅拟通信的用户容易接入,潜在窃听者也容易接入,因此安全问题总是同移动通信网络密切相关。不过安全问题涉及很广,移动通信业中的所有环节都需要考虑这个问题。本章将分别从业务提供商和用户两方面来讨论安全问题。移动通信已成为现代社会的一个组成部分,本章结尾还讨论了移动通信中的另一个问题:合法监听。

1G(第一代模拟移动通信网络)没有太多与安全有关的特性,并且当时的用户也不一定理解安全连接的意义。而今天的无线路径(它是系统中最不安全的部分)已经采取了非常有效的安全措施,但是这种做法有其自身的优缺点。如果无线连接是点到点的(两个用户之间),就可以使用专用的安全措施。军事通信中的无线连接就是采用这种方式。公众蜂窝网络中的无线路径基本上都是点到多点的(许多终端可以接收同一发射信号),这样,专用的安全系统就不太适用了。

GSM 的安全问题主要集中在无线路径安全上,即接入网络部分。对于 UMTS 网络来说,安全是个更大的主题。接入网连接自然必须安全,另外其他很多方面也需要安全。多种商业模型使得有些情形下敏感信息会在不同的网络部分以及不同的网络之间传输。很明显,这种情况下存在很严重的安全隐患。另外,地区和国际行政机构也在安全领域有各自的规定。UMTS 集成了电信业务和数据通信业务领域,这也对安全问题造成威胁。在 IP 领域,安全问题由来已久,人们已经认识到许多安全威胁并且发展了许多保护机制。

本章内容安排如下。9.1 节研究 UMTS 的接入安全。包括用户安全地接入到 UMTS 网络和接入网级的安全连接。UMTS 接入安全是建立在 GSM 接入安全模型基础之上的,但对其进行了一些增强。

在 9.2 节中,我们列举了一些 1999 版本的安全特性,其中有些继承自 GSM。

9.3 节处理网元层的安全问题。主要问题是如何保证 UMTS 网络内部连接的安全,以及不同运营商维护的网络之间的连接安全。由于 UMTS 核心网(3GPP R99)建立在 GSM 核心网基础上,它的安全部分和 2G 相比没有大的增强。在 UMTS 后续版本中,随着核心网的演进,情况发生了很多变化。9.3 节对所引入的机制进行简要的介绍。

9.4 节简单介绍了在业务的高层和内容提供商中的安全问题和机制。这些问题很大程度上独立于 UMTS 网络自身的结构，但是它们对整个系统的安全起着关键作用。本节还讨论了 UMTS 网络中 IP 多媒体子系统的接入安全。最后，9.5 节介绍在 UMTS 中如何满足合法监听的规定要求。

关于 UMTS 安全机制更详细的描述可以查阅 Niemi 和 Nyberg 的著作(2003 年)。

9.1 UMTS 接入安全

第三代移动通信网络的引入使无线接入技术从 TDMA 向 WCDMA 发展。尽管如此，但是对于接入安全的要求并没有改变。UMTS 仍需要对终端用户进行认证(即核查每个用户的身份)，没有人愿意为欺诈用户的呼叫付费。

RAN(无线接入网)提供对语音呼叫和发射用户数据的保密。这意味着用户可以控制和谁通信。用户还希望知道确实采取了保密，因此所采用的安全机制需要具有可见性。通常，保护用户位置的隐私性也是需要考虑的。一般人在大多数情况下并不关心是否有人能跟踪自己的行踪，但若发现自己一直被跟踪，就会非常恼怒。另一方面，用户的确切位置信息对于劫匪可能非常有用。同样，用户数据在网络中传输时，数据的隐私性也非常重要。在这里，隐私性和保密性大体上表示相同的含义。

对于付了费的用户而言，最重要的当然是 UMTS 接入的*可用性*。而对于网络运营商来讲，重要的是网络功能的*可靠性*：运营商需要通过控制网络内部以使其有效地工作。这一点是靠无线网络信令的*完整性校验*来保证的，所有的控制消息都要检查，看它是不是由授权的网元所产生。一般而言，完整性校验可以防止对消息进行篡改，如插入、删除或替换。

对网络运营商和用户而言提供安全的最重要手段是加密，它有各种不同的技术，源于*隐写术*这样一种科学和艺术。有时候我们需要通过密码和暗语等方式故意使通信内容无法被理解，这是保护信息不受恶意侵害的最有效方式。

9.1.1 2G 的遗产

从 1G 模拟系统向 2G 数字系统的转变使许多事情成为可能，其中包括先进的加密方法。GSM 系统中最重要的安全特性是以下几项。

- 用户鉴权。
- 无线接口中的通信加密。
- 临时识别码的使用。

随着 GSM 和其他 2G 系统越来越成功，这些基本安全特性的用处也变得越来越明显。制定 UMTS 安全方面标准时的主导原则自然也要把这些基本特性带到新的系统中。

GSM 的成功也凸显出它在安全方面的局限性。流行的技术也容易受到攻击。

GSM在安全方面受批评最多的是以下几项。

- 原则可以对网络进行主动攻击。任何人只要拥有所需的设备，就可以伪装为合法的网元或合法的用户终端(图9.1是一个实例)。
- 敏感的控制数据(如用于无线接口加密的密钥)在不同网络之间传输时没有加密。
- 安全体系中的某些部分没有公开(如加密算法)。这使外界无法用新技术对之进行分析，因而长期运行时能否信任就是一个问题。另外，全局加密早晚是一个趋势。
- 如果有人通过尝试所有可能密钥的方法来强力攻击的话，无线接口加密用的密钥将变得非常脆弱。

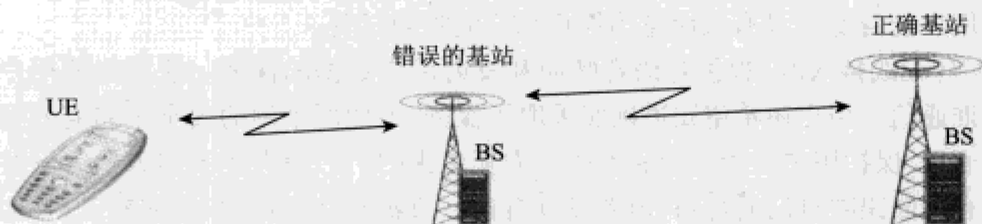


图9.1　主动攻击

GSM遗留了这些问题的原因是，与克服这些问题所增加的成本相比，这些问题造成的后果并不严重。然而，随着技术的进步，攻击者也会有更高级的工具。所以在3G中成本和安全性的比较就有了完全不同的结论。

UMTS针对GSM中的薄弱环节进行了发展。这也是3G安全体系设计的另一个主导原则。UMTS接入安全中最重要的特性如下。

- 用户和网络相互鉴权。
- 使用临时识别码。
- RAN加密。
- UTRAN内部信令的完整性保护。

其中加密和完整性保护采用广泛使用的加密算法，相互鉴权的算法由运营商决定。这些特性将在9.1.2节、9.1.4节、9.1.5节和9.1.6节具体描述。更详细的描述可参见3GPP标准文献TS 33.102。

9.1.2　相互鉴权

UMTS系统的鉴权机制包括三个实体。

- 归属网络。
- 服务网络(SN)。
- 终端，或者更确切地说是指USIM(通常是一个智能卡)。

相互鉴权的基本思想是，SN通过“质询响应”核查用户的身份(同GSM一样)，而

终端通过归属网络核查 SN。这后一点是 UMTS 相对于 GSM 新的特性，它使终端通过它可以检验是否连接到合法的网络。

相互鉴权协议本身不能阻止图 9.1 所示情况的发生，但结合其他安全机制后可以保证主动攻击者在此情况下得不到任何好处，它最多只能对连接产生干扰。然而，没有一种协议可以完全阻止这一类攻击，比如说，攻击者之一发射无线电干扰信号就能造成这种有害的后果。

鉴权机制的基础是 USIM 和归属网络数据库之间共享的主密钥 K，是一个长为 128bit 的永久密钥。密钥 K 在这两处永远都是不可见的，比如用户对自己的主密钥一无所知。

相互鉴权的同时产生了用于加密的密钥和用于完整性校验的密钥。这两个密钥是有相同的长度（128bit）的临时密钥。在每次的鉴权事件中，新的密钥从永久密钥 K 中得到。加密的基本原则是尽量减少永久密钥的使用次数，对大量数据的保护采用临时密钥。

现在我们在一般意义上对 AKA（鉴权和密钥协商机制）进行讨论。服务网络识别用户后就可以开始鉴权过程。用户识别在识别码（永久识别码 IMSI 或临时识别码 TMSI）发送到 VLR 或 SGSN 后进行。然后 VLR 或 SGSN 向归属网络的 AuC（鉴权中心）发送鉴权数据请求。

AuC 有用户的主密钥，它根据 IMSI 的信息产生用户的鉴权向量。鉴权向量的生成过程涉及一些加密算法，这些算法在 9.13 节中有更为详细的描述。这些产生的向量在鉴权数据响应中送回 VLR/SGSN。图 9.2 示出了这个过程，这些控制消息通过 MAP（移动应用部分）协议传输。

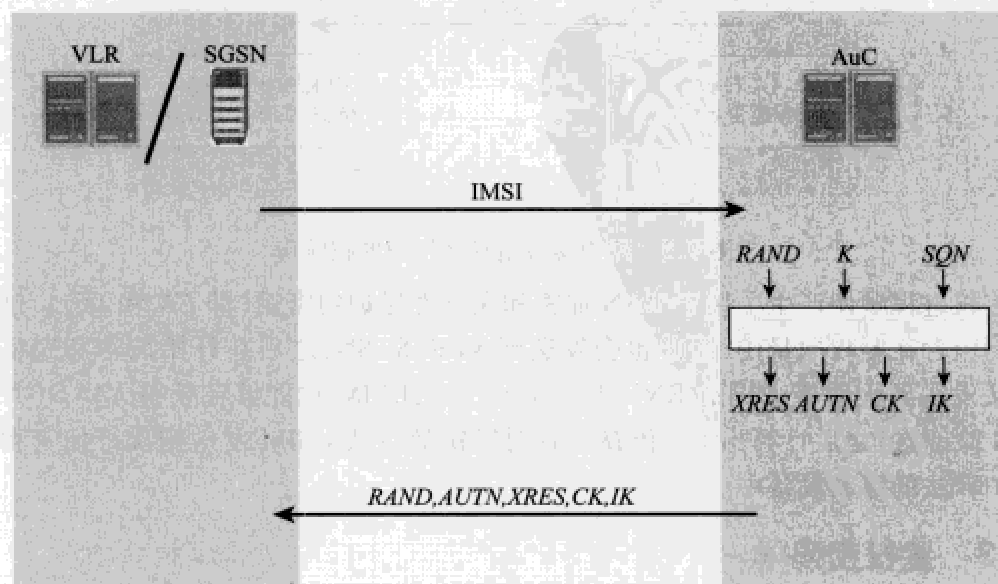


图 9.2 鉴权数据请求和鉴权数据响应

在服务网络中,每个鉴权实例(也就是每次鉴权过程的执行)需要一个鉴权向量。这意味着,并不是每一次鉴权事件都需要有 SN 和 AuC 之间的信令,这个信令可能是长距离的,原则上可以不管用户的行为,只在初始注册时进行。实际上,VLR/SGSN 可以在存储的向量用完之前从 AuC 取出新的鉴权向量。

服务网络(VLR 或 SGSN)向终端发送*用户鉴权请求*,其中包含鉴权向量中的两个参数“RAND”和“AUTN”。这些参数传送到任意一个存有 USIM 的抗篡改环境中(如 UMTS 集成电路卡 UICC)。USIM 包含主密钥 *K*,它用 *K*、*RAND* 和 *AUTN* 作为输入参数,按与 AuC 中产生鉴权向量相似的方式进行计算,这个过程和相应的 AuC 计算一样要涉及几个算法的执行。计算的结果能使 USIM 验证出参数 AUTM 是否真的是由 AuC 产生的,如果是就通过*用户鉴权响应*向 VLR/SGSN 发回 *RES* 参数。然后 VLR/SGSN 把用户响应的 RES 和它所期望的响应 XRES(鉴权向量的一部分)进行比较。如果匹配,鉴权顺利通过。图 9.3 示出了这部分的处理过程。

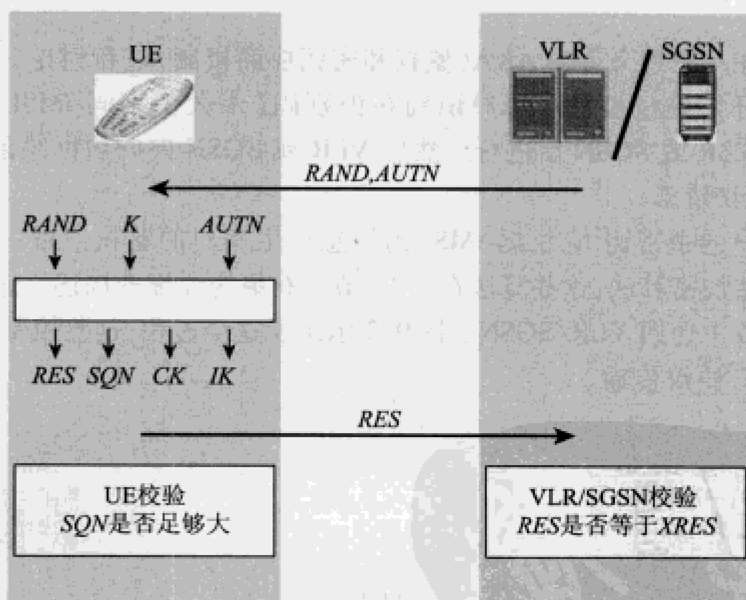


图 9.3　用户鉴权请求和用户鉴权响应

鉴权过程顺便产生了用于 RAN 加密和完整性保护的密钥(即 *CK* 和 *IK*)。这些临时密钥包含在鉴权向量中,因此也会发送到 VLR/SGSN,之后在开始加密和完整性保护时又发送到无线接入网的 RNC 中。在另一端,USIM 也能够在获得 *RAND*(并通过 AUTN 验证它)之后计算出 *CK* 和 *IK*。临时密钥随后从 USIM 发送到执行加密和完整性保护算法的移动设备中。

9.1.3　鉴权密码学

下面我们进一步来看 AuC 中的鉴权向量的产生。图 9.4 是该过程更详细的说明。该过程以选择正确的序号 *SQN* 作为开始。简单地说,序列号应以升序方式来选择。使

用序列号的目的是为了以后让用户认识到所产生的鉴权向量是新的(即以前没使用过)。选择序列号的同时产生一个 128bit 长的随机比特串 *RAND*。这并不是件容易的事情,不过我们在这里只是假定有一个用于加密的伪随机数发生器,如果有良好的物理随机源可作为种子,这个伪随机数发生器就能生成大量的随机输出比特。

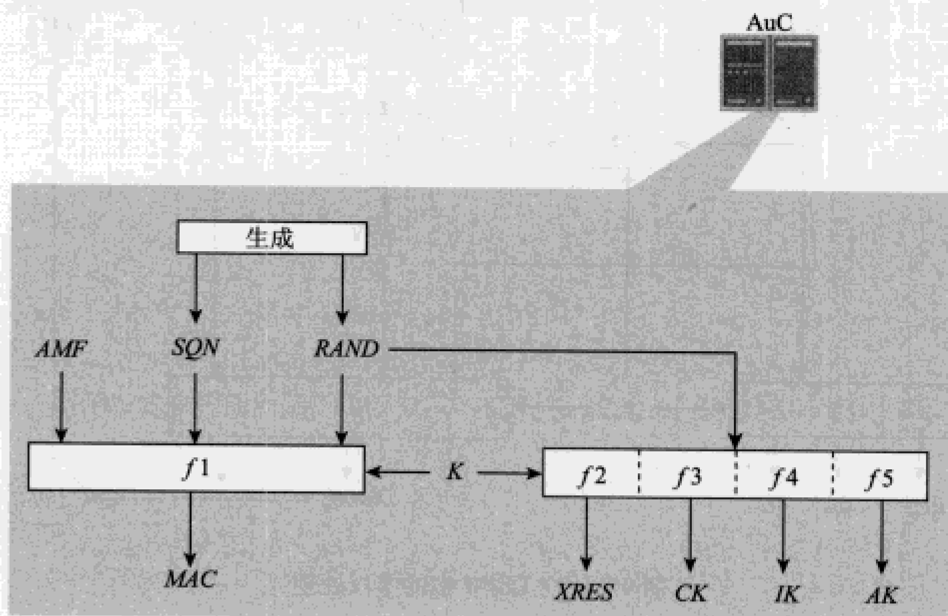


图 9.4 鉴权向量的产生

计算鉴权向量的关键是单向函数。它是一种能够简单计算,同时在实际当中又不可能求逆的数学函数。换句话说,如果给定输入参数则存在快速算法可计算出输出参数,而当已知输出时,并没有有效的算法能计算出相应的输入。当然,一种简单的方法是尝试所有可能的输入,直至找到某个输入能产生所需要的输出。很明显,随着输入长度的增加,这种穷举搜索的算法将极其低效。

计算鉴权向量总共使用了五个单向函数,分别用 *f*1、*f*2、*f*3、*f*4、*f*5 表示。*f*1 和其他四个的不同处是它有四个输入参数:主密钥 *K*、随机数 *RAND*、序列号 *SQN* 和鉴权管理字段 *AMF*。*f*2 ~ *f*5 这四个函数只用 *K* 和 *RAND* 作为输入参数。这五个函数都要求有单向特性,它们都可以用同一个核函数建立。不过它们之间有这样一种基本区别:从一个函数的输出不可能获得有关其他函数输出的任何信息。*f*1 函数的输出是 *MAC*(消息鉴权码,64bit),*f*2、*f*3、*f*4、*f*5 的输出分别是 *XRES*(32 ~ 128bit)、*CK*(128bit)、*IK*(128bit)和 *AK*(64bit)。鉴权向量由参数 *RAND*、*XRES*、*CK*、*IK* 和 *AUTN* 组成。AUTN 是串接三个参数后得到的,就是把 *SQN* 逐比特加到 *AK*、*AMF* 和 *MAC* 上。

现在我们来进一步研究 USIM 端的鉴权处理,图 9.5 示出了这一过程。这一端的鉴权也同样用到了相同的 *f*1 ~ *f*5 这五个函数,但是顺序略有不同。*f*5 必须在 *f*1 之前计算,因为 *f*5 用于隐藏 *SQN*。这是为了防止窃听者通过 *SQN* 获得用户身份的有关信

息。*f*1 的输出在用户端标记为 *XMAC*。从网络收到的 *AUTN* 参数包含 *MAC*。如果 *XMAC* 和 *MAC* 匹配，说明 *RAND* 和 *AUTN* 是由已知 *K* 的同一实体创建的，即是由用户网络的鉴权中心创建的。

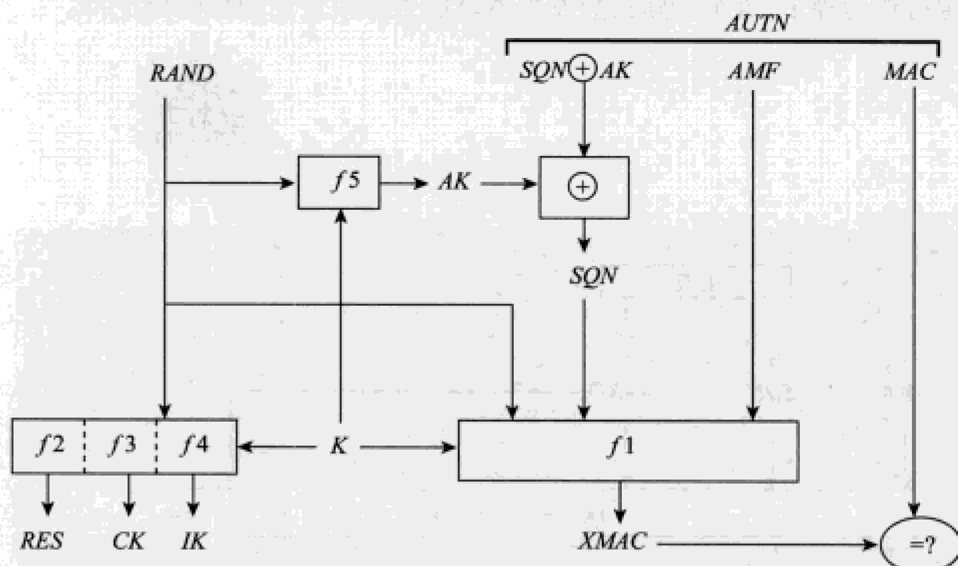


图 9.5　在 USIM 中的鉴权处理

然而还有一种可能是攻击者记录了先前的鉴权事件，再次使用其中的 *RAND* 和 *AUTN*。前面所说的序列号能够防止这种威胁。USIM 只需简单地检查它先前是否收到过同样的 *SQN*。最简单的检查方法是要求 *SQN* 升序排列。也有一种可能是 USIM 允许一些 *SQN* 不按顺序到达。此时它应维持一个尽量短的列表，其中包括迄今为止接收到的最大序号。鉴权向量需要从鉴权中心传送，鉴权向量的使用又是独立进行的，这些原因使得使用时的向量和当初产生的向量顺序不一致。最明显的情形是 PS 域和 CS 域的移动性管理功能是相互独立的，因此鉴权向量分别到达 VLR 和 SGSN，其使用也是独立的。

算法 *f*1 ~ *f*5 原则上由运营商确定。因为这些算法只在同一个运营商的鉴权中心和 USIM 中使用。3GPP TS 35.206 标准中有一个示例的算法集，称为 MILENAGE。序号管理原则上也取决于运营商。有两种基本的编号方案：按每个用户编号或者按一个全局计数器（如世界时）来编号，也可以联合使用这两种方法，比如 *SQN* 的高位按用户编号，低位按全局计数器编号。

相互鉴权机制基于同时存储在 AuC 和 USIM 中的两个参数：静态的主密钥 *K* 和动态的序列号 *SQN*。在通信两端保持这些参数的同步非常重要。这一点对静态主密钥 *K* 非常简单，但 *SQN* 的动态信息可能会由于某种原因而失步，其结果会造成鉴权失败。再同步过程就是为了解决这个问题（如图 9.6 所示）。以主密钥 *K* 为安全通信的基础，USIM 把当前的 *SQN* 通知给 AuC。

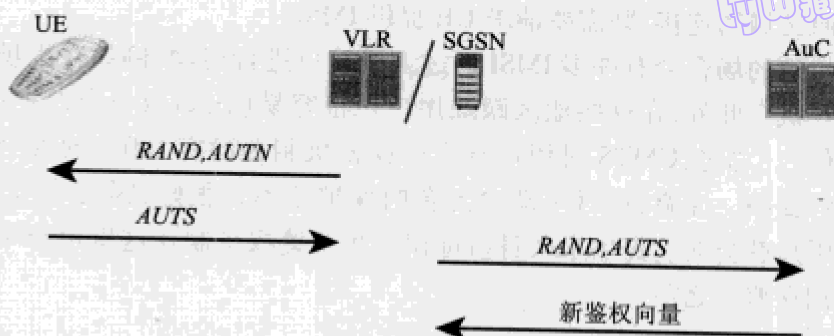


图 9.6 再同步过程

再同步期间提交一个参数 *AUTS*。它包含两个部分:隐藏于 *AK* 中的 *USIM* 序列号和消息鉴权码 *MAC-S*,这个码由另一个单向函数 $f1^*$ 利用输入参数 *SQN*、*K*、*RAND* 和 *AMF* 计算出。从失败的鉴权事件可以获取参数 *RAND* 和 *AMF*。单向函数 $f1^*$ 必须与函数 *f1* 不同,否则,所记录的 *AUTN* 原则上可以作为再同步中的有效 AUTS 参数,这样攻击者至少能对鉴权机制进行干扰。

9.1.4 临时标识码

在 UMTS 中,用户的永久标识码是与 GSM 网络一样的 IMSI。不过 UTRAN 对用户的鉴别大多采用临时标识码:CS 域用 TMSI,PS 域用 P-TMSI。这样对于被动的窃听者,用户的身份基本上总能得到保密。例外的情形是初始注册,这时网络还不知道用户的永久标识,所以用不了临时标识。在此之后原则上就可以使用临时标识了。

临时标识码的工作原理如下。假定 SN 已经根据 IMSI 识别出了用户。然后 SN(VLR 或 SGSN)给用户分配一个临时标识(TMSI 或 P-TMSI)并维护临时标识和永久标识间的映射。临时标识仅对本地有效,每个 VLR 和 SGSN 只需注意不要把相同的 TMSI/P-TMSI 同时分配给两个不同的用户。一旦要进行加密,就把分配的临时标识发送给用户。在网络分配新的临时标识 TMSI 或 P-TMSI 之前,在上下行链路的信令中都一直使用这个临时标识。

新的临时标识的分配由移动终端确认,此后旧的标识就从 VLR(或 SGSN)中删除。如果 VLR/SGSN 没有收到移动终端的分配确认,则同时保存新旧两个临时标识,并且在上行链路中两者都可以接受。下行必须使用 IMSI,因为网络不知道当前终端存储的是哪个临时标识。此时 VLR/SGSN 通知终端删除所有存储的 TMSI/P-TMSI,随后重新分配。

还存在一个问题:SN 开头如何获得 IMSI? 由于临时标识仅在本地有意义,因此必须要附加上本地区域的标识码,以使用户有明确的标识。TMSI 附加了 LAI(位置区标识码),PTMSI 附加了 RAI(路由区标识码)。

当 UE 到达一个新的区域时,如果新地区知道原地区的地址(指 LAI 和 RAI),IMSI 和(P-)TMSI 间的关联可以从原来的位置区或路由区获得。如果原位置未知,或者

无法建立与原区域的连接，则需要请求 UE 提供 IMSI。

在一些特殊的场合会有许多 IMSI 通过无线接口进行传输，例如在机场，人们会在飞行结束后开机。此外，在这些地区跟踪用户也很容易（比如当一个人走出飞机时就能确认出身份）。总之，UMTS 对用户身份的保密机制并没有 100% 的安全，但它提供了相对较好的保护。注意，针对主动攻击者的保护还不是很好，因为攻击者可以假装成一个 SN，用户就会向它提供永久身份标识。相互鉴权机制在这里也帮不上忙，因为用户身份识别在鉴权之前。

9.1.5 UTRAN 加密

一旦用户和网络完成了相互的鉴权，就可以开始安全通信。如前所述，鉴权成功后，*CK* 在核心网和用户终端之间共享。在加密开始之前，通信双方要对使用的算法达成一致。所幸的是 3GPP R99 只定义了一种算法。加密和解密在移动终端和网络侧的 *RNC* 中进行。因此 *CK* 必须要从 CN 传输到 PAN。这一点由一个 RANAP（RAN 应用部分）消息完成，该消息称为“安全模式命令”。RNC 获得密钥 *CK* 后向终端发送 RRC 安全模式命令，从而打开加密。

UMTS 的加密机制基于图 9.7 所示的流加密的概念。明文与一个伪随机的掩码数据逐位相加，掩码是根据密钥 CK 和其他一些参数获得的。这种加密的优点是：掩码可以在明文之前产生，最后的加密是非常快的位操作。接收端的解密过程完全相同，因为掩码比特加两次和加 0 的效果一样。

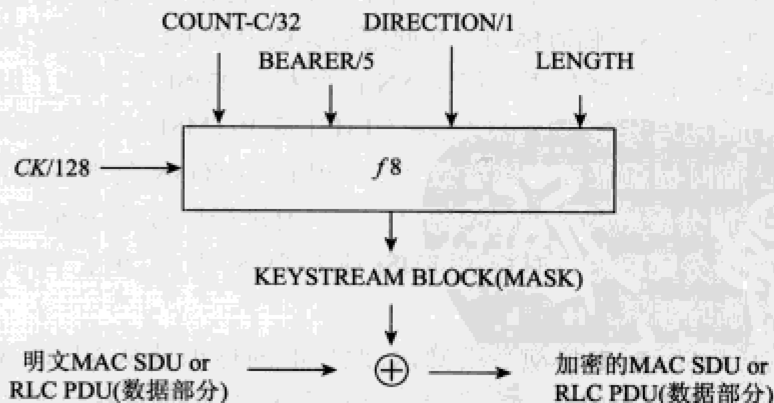


图 9.7 UMTS 中的流加密

由于掩码不依赖于明文，所以还必须要有另一个输入参数，该参数在新的掩码生成时就变化一次。否则两个不同的明文（P1 和 P2）将由同一个掩码保护。于是就会出现下面这种不期望的现象：如果将 P1 和 P2 逐位相加，再对加密后的结果也逐位相加，所得的比特序列完全相同。这也是由于两个相同的掩码逐位相加后相互抵消。因此，在无线接口窃听加密消息的任何窃听者都可以得到 P1 和 P2 位相加的和。典型的情况是，如果两个有意义的数据逐位相加，有可能从结果中得出这两个数据，意味着两个

消息 P1 和 P2 的加密被破解了。

加密在 MAC(媒体接入控制层)或 RLC(无线链路层)进行。这两种情况都有一个随每个 PDU 变化的计数器。在 MAC 层叫 CFN(连接帧号),在 RLC 层则是一个特定的 RLC-SN(RLC 序列号)。如果以这些计数器作为掩码生成时输入参数,前面提到的这种问题还会存在,因为计数器很快就会循环回来。因此引入了称为 HFN(超帧号)的长计数器。每当短计数器(MAC 中的 CFN 和 RLC 中的 RLC-SQN)计数循环一周时 HFN 增加。HFN 和短计数器的组合叫 COUNT-C,用作掩码生成时不断变化的输入参数。

原则上,长计数器 HFN 最终也将循环一周。不过每当 AKA 过程产生新的密钥时,长计数器就会复位。鉴权事件发生的频率很高,足以避免 HFN 计数循环。

因为不同的无线承载的计数器是相互独立的,所以加密算法也需要无线承载标识 BEARER 作为输入。如果不使用 BEARER 作为输入参数,又将出现相同输入参数送给算法,相同的掩码将生成多次。这样就可能发生前面提到的问题,用相同掩码加密的不同消息(不同的消息在不同的无线承载上)将会暴露给攻击者。

加密机制的核心是函数 *f*8 表示的掩码生成算法。已经公开的规范是 3GPP TS 35.201,这种算法基于一种新的分组加密技术,称为 KASUMI(3GPP 对此有另一个规范 TS 35.202)。这个分组加密算法把 64bit 的输入转变成 64bit 的输出。转换由 128bit 的密钥 *CK* 来控制。如果 *CK* 未知,就不可能以有效的算法从输出计算出输入或者相反。原则上,只有满足下面的条件之一时才可能转换。

- 尝试所有可能的密钥,直到找到正确的密钥。
- 以某种方式收集一个巨大的表,它包含所有 2^{64} 个输入输出对。

在实际中,这两种方法显然都是不可行的。

有可能在连接开始时鉴权还未执行。此时用前一次的密钥 *CK* 来加密。在两次连接这间,密钥存储在 USIM 中。另外,到目前为止使用过的最大 HFN 的高位存储在 USIM 中。对于下一个连接,存储的值加一,并且作为 HFN 高位的起始值。

终端用加密指示符向用户表明是否进行了加密,从而提供了加密机制的可见性。注意,虽然强烈建议使用加密,但是对于 UMTS 网络,加密仍是可选的。

9.1.6 RRC 信令的完整性保护

完整性保护的目的是对单个控制消息进行鉴权。其重要性在于,单独的鉴权过程只能保证鉴权当时通信双方的身份。可用图 9.1 来说明这一点:一个"中间人"(仿冒造的基站)作为简单的中继以正确的形式传送所有消息,直到鉴权过程全部完成。之后,这个中间人就可以随意篡改消息。如果每个消息都是单独保护的,就能发行对消息的有意篡改,伪造的消息会被丢弃。

完整性保护在 RRC 层执行。同加密一样,用在 RNC 和终端之间。完整性密钥 *IK* 在 AKA 过程中产生,也和 *CK* 类似。另外,*IK* 和 *CK* 一起以安全模式命令传送到 RNC。

完整性保护机制基于MAC(消息鉴权码)的概念。这是一个由秘密密钥*IK*控制的单向函数。这个单向函数用*f9*表示,它的输出是MAC-I:一个32bit的伪随机比特序列。MAC-I附加在每个RRC消息后,在接收端也要生成MAC-I并进行校验。任何输入参数的变化会以不可预见的方式影响MAC-I。函数*f9*示于图9.8。它的输入是*IK*、RRC消息、计算器COUNT-I、方向位(上/下行链路)和一个随机数*FRESH*。COUNT-I参数类似于加密中用的对应的计数器,其高位是HFN,低4位是RRC-SQN。总而言之,COUNT-I防止以前用过控制消息再次出现:它能确保完整性函数*f9*的每一次运行都有不同的输入参数。

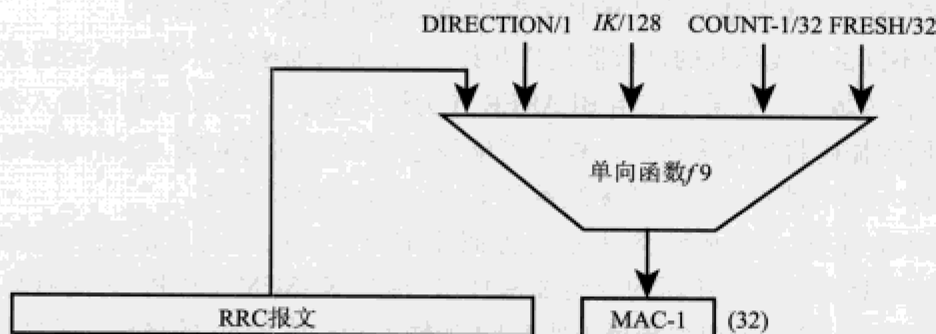


图9.8 MAC

参数*FRESH*由RNC选择,并发送给UE。需要防止恶意选择COUNT-I的初始值。前面指出,连接之间*HFN*的高位存储在USIM中。攻击者可以伪装成USIM向网络发送伪造的值以强迫*HFN*的初始值非常小。鉴权过程没有执行的时候用旧的*IK*。如果没有*FRESH*这个参数,攻击者就可以用记录的MAC-I值重放以前连接的RRC信令消息。通过随机选择*FRESH*,RNC就可以防止这类基于以前记录的连接信息而进行的重放攻击。正如已经解释的,*FRESH*激活时,始终递增的计数器COUNT-I可以防止这种重放攻击。注意,虽然无线承载标识是加密算法的一个输入参数,但不是完整性算法的输入。控制面也存在多个并行的无线承载,这似乎为控制消息的重放提供了可能,这些控制消息是在同一RRC连接的不同无线承载上记录的。不过情况并非如此,因此计算MAC时总要附加无线承载标识(虽然它不随消息传送)。因此,无线承载标识对MAC-I的值有影响,我们已经防止了根据不同无线承载的记录所进行的重放攻击。

这种机制虽然不能保护个别RRC控制消息的完整性。实际上,在完整性钥*IK*生效之前发送的消息就不能受到保护。典型的例子是RRC连接请求消息。

完整性保护的算法基于与加密算法中相同的核函数。KASUMI分组加密以一种特殊的模式用来来建立MAC函数。

由于性能的原因,UTRAN中的完整性保护机制没有用在用户平面中。另一方面,还有一个特别的完整性保护控制平面过程用于周期性本地鉴权。该过程检验RRC连接期间发送的数据量。因此,用户发送的数据量受到了完整性保护。

9.1.7 接入安全总结

本节对最重要的接入安全机制及其相互关系给出一个图示性的归纳。为了清楚的原因，许多参数没有在图 9.9 中示出。比如 *HFN* 和 *FRESH* 是在不同网元之间传送的重要参数，但图中省略了它们。

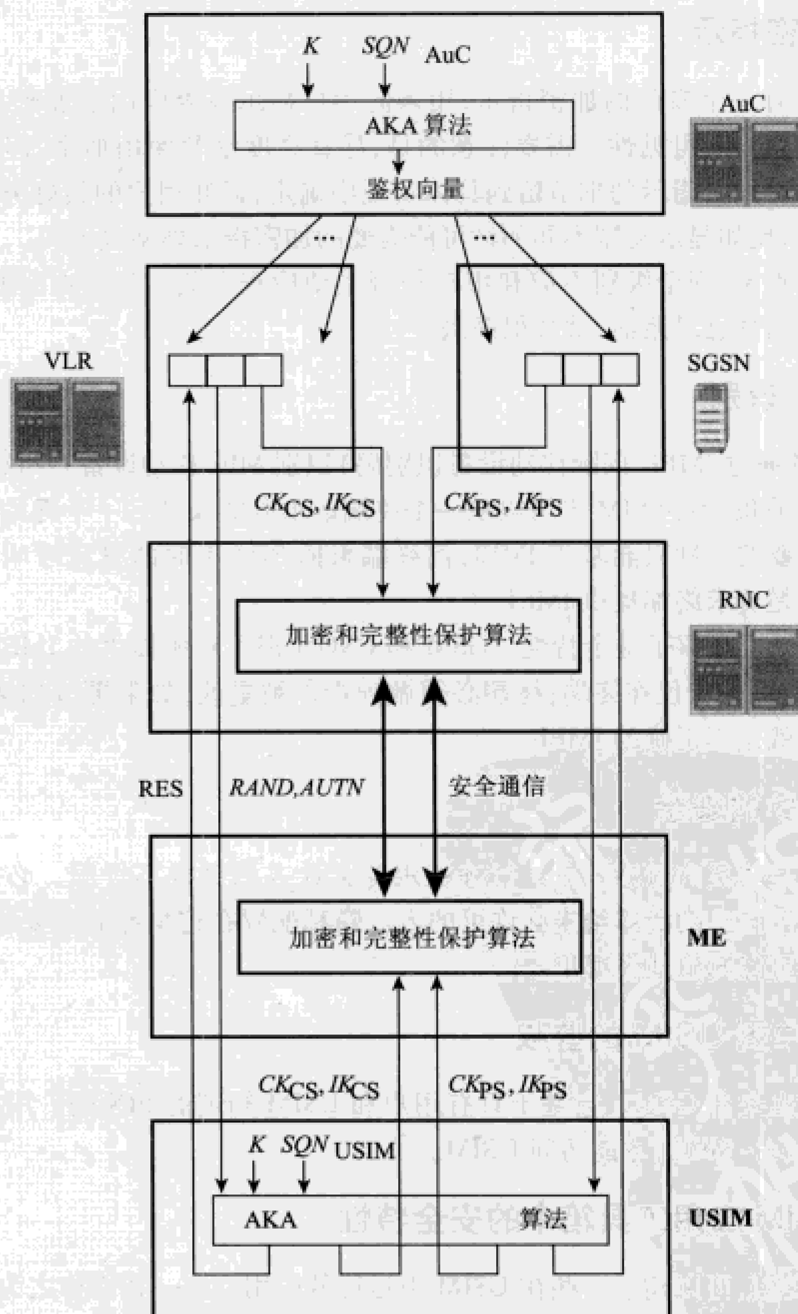


图 9.9 UMTS 接入安全总结

9.2 3GPP R99中的辅加安全特性

3GPP R99标准还有一些补充的安全特性，其中一些是首次加入到3GPP R99，另一些则是直接从GSM网络中继承下来的。

9.2.1 加密指示

在ME中有一个专门的加密指示，用来向用户显示是否应用了加密，这样就可以使安全机制对用户有可见性。需要注意的是，尽管高度推荐使用加密，但在UMTS中加密是可选的。加密指示的细节留到具体实现中确定，通知用户的最好方式与终端的特性关系很大，比如显示类型不同的话可能需要的加密指示类型也不同。

重要的一点是，安全级别不应和用户是否主动检查有关。只是在有些时候，用户若能看到安全属性已经激活，就会很高兴。

9.2.2 UE识别

GSM系统通过IMEI（国际移动设备识别码）识别ME（移动设备）。这个识别码并不直接与用户关联，因为SIM卡可以从一个终端取出后放入到另一个终端中。不过网络中有一些重要的特性只能基于IMEI，例终端未插SIM卡时的紧急呼叫。此时仅有的识别方式就是要求终端提供IMEI。

UMTS系统也保留了这个特性。GSM和UMTS都不对所提供的IMEI进行鉴权。因此对IMEI的保护仅仅在终端：终端必须做到难以被更改，如果更改的话，网络发出请求时提供的就是不正确的IMEI。

9.2.3 LCS的安全

用户位置是明显的敏感信息。行迹被跟踪会让人感到极不舒服。必须要有安全机制来防止位置信息的泄露给未必许可的人。隐私配置在这里起着重要的作用，用户必须能决定谁可以知道他在哪里。

9.2.4 用户到USIM的鉴权

这个特性也来自GSM。它基于只有用户和USIM知道的PIN码。用户必须提供正确的PIN码（4～8bit），才能访问USIM。

9.2.5 USIM应用工具箱中的安全特性

和GSM类似，可以建立一些在USIM中运行的应用。这一特性称之为（U）SIM应用工具箱。其目的部分是为了让归属运营商能直接发送消息到USIM。它也进一步规定了消息传送的保护类型。保护机制的许多细节都与具体实现有关。

9.3 系统级和网络级的安全

本节简单讨论网络级的潜在安全威胁以及保护方法。其目的是保护网元间通信的保密性和完整性。这些网元可以属于同一个网络也可以属于不同的网络。后一种情况尤其需要完全标准化的安全方案以保证互操作性。

3G 商业链由四部分组成:用户、载波提供商、服务提供商和内容提供商,如图 9.10 所示。用户付费使用的服务涉及这条链中的各部分:载波提供商提供建立连接的平台,服务提供商安排 USIM(身份信息)和实际的服务,内容提供商负责业务所请求的内容。载波提供商、服务提供商和内容提供商可能是同一个公司的,但也不一定必然如此。在 GSM 中,实际存在着这三方的各种组合。很明显,用户因其使用的服务交费,商业链中的其他各方分享收入。在载波、服务和内容提供商之间传输的财务信息是非常敏感的信息,因此控制财务信息流传送的系统面临潜在的安全威胁。

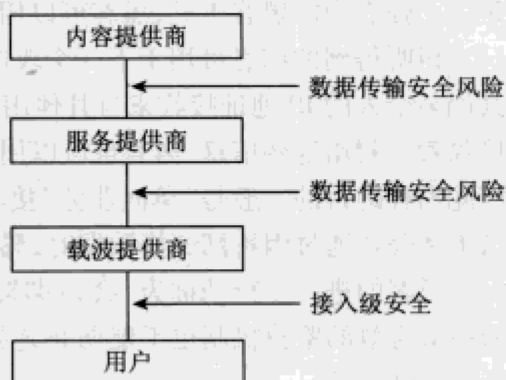


图 9.10 商业链中的安全隐患

9.3.1 典型的安全攻击

针对 UMTS 网元间通信的威胁许多同应用层的威胁是类似的。虽然应用与应用之间有很大差别,但所有情形都应考虑本节给出的攻击示例。

进行安全攻击的方式非常多,只受到想象力和有效保护的限制。下面列出了一些例子,请注意这只是其中的一部分。

- 社会工程。
- 电子窃听(嗅探)。
- 欺骗。
- 会话篡改。
- DoS(拒绝服务)。

虽然社会工程在许多攻击中起着重要作用,但普通用户一般并不认为这是安全问题。对于用户而言,社会工程可能意味着以某种方式获取对终端的访问,即以某些方式获得 PIN 码。为了防止社会工程,用户可以记住 PIN 码,并在终端激活时要求输入 PIN 码。社会工程在网络一侧也非常普遍。运营企业的工作人员经常会接到一些奇怪的电话,说他需要某个设备的用户 ID 和密码,因为负责这个设备的人去渡假了或者联系不到。这样的电话经常就是社会工程,是坏人想窃取安全信息。实际上,黑客通常都是首先试这种办法。其结果是,社会工程使得攻击者能够进入一些重要的或者不太重要网元。在 IP 领

域，社会工程已经比较普遍，但是在通信领域它还没有成为常见的攻击方式。这主要是因为通信设备并不是公众可以接入的，工作人员的责任心也很强。

电子窃听也称为嗅探，是另一种常见的攻击方法，9.1.1节和9.1.5节已经做了介绍。这种方法很难发觉，在物理上也难以防止。黑客试图通过窃听搜集用户ID和密码等信息。糟糕的是，任何人都可以在因特网上找到并下载到窃听软件。窃听程序本身只是一种工具，在好人的手里它用来进行网络监测和故障检测。落在坏人手里，就是一个强有力的黑客工具，黑客可以用它悄悄监测大量的因特网连接。

窃听得到的信息可用于下一个攻击手段，称为"欺骗攻击"。它可以使攻击者能用其他某个人的IP地址接收来自其他用户的信息包。也即，攻击者代替了连接中的正确接收者。利用这些信息，黑客也可以用别人的IP地址打开连接，不过这样做比较困难。因此黑客的目的一般是"单向业务"接收。人们现在要花很多时间在家里远程工作，当员工和公司通过因特网交换数据时，黑客就可以访问公司的信息。

黑客的进一步行动称为"会话绑架"，企图占用现有的连接。前面已经提到，即使采用最有效的鉴权机制也不能防止连接建立以后被绑架。我们需要在整个会话中进行完整性保护。

在DoS的攻击中，黑客的目的不是收集信息，而是妨碍其他用户和服务提供者。在典型的DoS攻击中，攻击者生成"干扰"业务，在最坏情况下能阻塞目标服务器，使之无法再提供服务。DoS的思想就是用大量请求填满服务器的服务请求队列，并忽略服务器返回的所有响应。因此，服务器为了一个不会发生的呼入连接浪费了资源。当连接超时时，时分的资源又被另一个连接占用。不断用这些新的请求填满容纳连接尝试的缓冲区时，服务器就一直被这些请求阻塞，无法提供"真正"的服务。

不幸的是还有很多更复杂的DoS攻击，因特网上有许多用于DoS攻击的工具。总而言之，防止DoS攻击是非常困难的。

高级的DoS攻击可能与前面提到的方法结合。比如，DoS可由一个"盗取"的IP地址发起，在分布式方式下可以使用成百上千的计算机参与DoS攻击。DoS是一种危险的而又强大的攻击方式，很容易带来巨大的经济损失。

前面简单介绍了最常见的安全攻击。由于这些攻击工具可以从因特网上免费下载，所以这些威胁不容忽视。那么怎么才能消除这种危胁呢？安全应该看成一个链，整个系统（即通信安全、数据安全、信令安全）的健壮性取决于最薄弱的链路。也就是说，所有的都必须是安全的，包括算法、协议、链路、端到端的路径、应用等。

9.3.2　3GPP网络域安全概述

前面已经提到，GSM网络安全体系的一个弱点是鉴权数据没有经过保护就在不同的网络间传输。例如CK用来保护无线接口，但是CK本身在网络之间传输时却没有经过加密处理。其主要原因在于SS7网络的封闭特性：只有少量的大机构能访问SS7网络。UMTS R99中的核心网结构与GSM差不多，因此核心网之间的业务安全没有

得到太大增强。

在 UMTS 的后续版本中,CN(核心网)的结构有了演进,IP 协议成为网络层的主要协议。虽然这并不意味着不同 CN 之间的信令要在真正的开放式连接上传输,但访问 CN 业务确实变得更为容易。我们所面临的新问题是,这样的通信结构涉及更多的参与者,还存在 IP 方面经验丰富的黑客群体。

保护网络域业务的基本工具是 IPSec 协议。它提供了 IP 层通信的保密性和完整性。通信双方也可以使用 IPSEC 进行相互鉴权。这其中的关键问题是密钥管理:即如何产生、交换和分配用于保密和完整性保护算法的各种密钥。9.3.3 节将简单介绍 IPSec。

除了保护基于 IP 的网络,UMTS 版本 4 也加强了对纯 SS7 网络的安全保护。特别是为 MAP 协议开发了一种专用的安全机制,叫作 MAPSec,它可以提供保密性和完整性保护。

9.3.3 IPSec

IPSec(IP 安全)是由 IETF(Internet Engineering Task Force)进行标准化的。它由许多个请求说明(RFCs 2401 - 2412)组成,是 IPv6 不可缺少的一部分。在 IPv4 中,IPSec 作为可选的插件来提供 IP 层的安全。IPSec 的主要组成部分是以下几项

- AH(鉴权头)。
- ESP(封装安全负荷)。
- IKE(因特网密钥交换)。

IPSec 通过 ESP 和/或 AH 达到保护 IP 包的目的。简单地讲,ESP 能同时提供保密性和完整性保护,AH 仅提供完整性保护。两者有很多区别,又有大量重叠。IPSec 包含这种冗余的原因之一是出口控制:大多数国家的保密机制的出口受到严格控制,而完整性保护机制的出口则不受限制。目前,这种限制已经去掉,因此 AH 相对于 ESP 的重要性有所下降。

AH 和 ESP 都需要密钥。但更一般地说,SA(安全关联)的概念对 IPSec 更为重要。SA 不仅包含加密和鉴权密钥,还包含所使用的算法、密钥及 SA 的生存期。SA 也包含防止重放攻击的 SQN 等信息。

在使用 AH 和 ESP 之前,必须先要协商每个通信方向上的 SA。这种协商是用 IKE 协议以安全的方式进行的。有几种不同的 IKE 模型,它们的想法是一样:通信双方产生"工作密钥"和 SA,然后用于保护后面的通信。IKE 基于公钥加密这种天才的思想,它可以在不安全的信道中交换安全通信所需的私钥。不过,如果没有长期的密钥,就不能对使用 IKE 的通信方进行鉴权。一般有两种方法,一种是手工交换机密,或者是采用 PKI(公开密钥设施)和证书。两种方式都不简单,前者需要做大量的配置工作,后者需要有特定功能的专用设施。

IKE 决定的 SA 协商与其用途无关。因此 IKE 也可以用于比如 MAPSec 等中的密

钥协商和SA。

在结束本节之前，我们现在对ESP稍做介绍。ESP模式有两种，即传输模式和隧道模式。在传输模式下，IP包中除了IP头以外的部分都要进行加密。然后在IP头和加密部分之间增加新的ESP头，新的ESP头包含所用SA和ID等信息。另外，加密过程一般会在包尾增加一些比特。最后，按除IP头以外的所有部分计算出MAC(消息鉴权码)，并把它附加到包的最后。接收端首先验证完整性。做法是先去除头部的IP头和尾部的MAC，根据ESP头得到密钥和算法，然后对包的剩余部分计算MAC，最后把计算结果同包中的MAC进行比较。如果完整性检验的结果通过，则去掉ESP头并对剩余部分进行解密，解密也是基于ESP头中的信息。具体原理可参见图9.11。

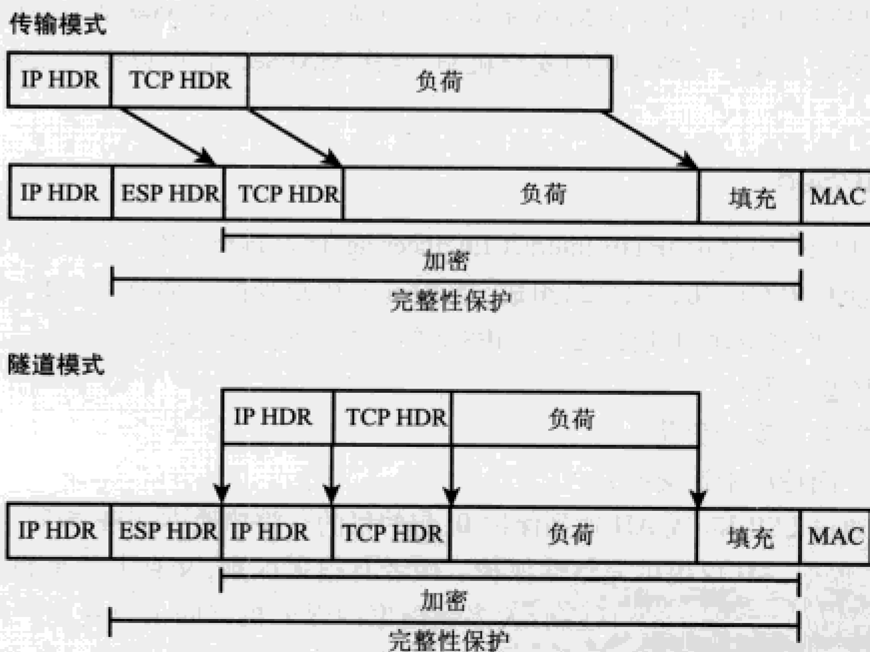


图9.11 安全负荷封装ESP

隧道模式不同于传输模式的是，它对包增加一个新的IP头，然后再按照传输模式的方式处理。这样就能保护原始包的IP头，见图9.11。

传输模式是在两个端点间使用ESP的基本模式。不过在3GPP中使用传输模式时，还存在着两个问题。

- 通信的网元必修知道彼此的IP地址。
- 通信网元能实现所有的IPSec功能。

隧道模式的典型应用是VPN(虚拟专用网)。IPSec用在两个中间节点(安全网关)间。网关之间受保护的包包含着端到端的数据包，因此这样就间接地提供了端到端的保护。很显然，在这种情况下，每个网元都要信任彼此的网关。另外，从端点到网关的这部分要用其他方法保护(比如物理保护)。UMTS核心网控制消息首选的保护方法是在安全网关之间使用隧道模式的ESP。基于安全网关和IPSec属性的网络域安

全结构详情请查阅 3GPP TS 33.210。在 R6 中,3GPP 规定了 PKI 机制在 3GPP 环境中的用法,以支持网络域安全机制(见 TS 33.310)。

9.3.4 MAPSec

本节简单讨论 MAPSec 的基本特性。基目的是保护 MAP 操作的保密性和完整性。MAPSec 保护模式 2 同时提供了机密性和完整性,而 MAPSec 保护模式 1 只提供完整性保护,MAPSec 保护模式 0 则不提供任何保护。

MAPSec 的基本功能如下。将明文 MAP 消息加密后放入另外一个 MAP 消息中的"容器"中。新的 MAP 消息同时包含一个覆盖原始信息的加密校验(即 MAC)。使用加密技术和 MAC 需要有密钥。MAPSec 借鉴了 IPSec 中的 SA 概念。SA 不仅包括密钥也包括一些其他相关的信息(如密钥的生存期和算法标识)。MAPSec SA 和 IPSec SA 类似,但不完全相同。

支持 MAPSec 的密钥管理计划采用类似于 IPSec 中的技术,3GPP R6 尚不包含这些机制。

9.4 应用和服务的保护

网络的安全是根据 OSI(Open System Interconnection,开放系统互连)模型来实现的,即每个 OSI 层都有各自的安全保护的方式,如图 9.12 所示。安全保护有两个主要分支,即逐链路的安全和端到端的安全。

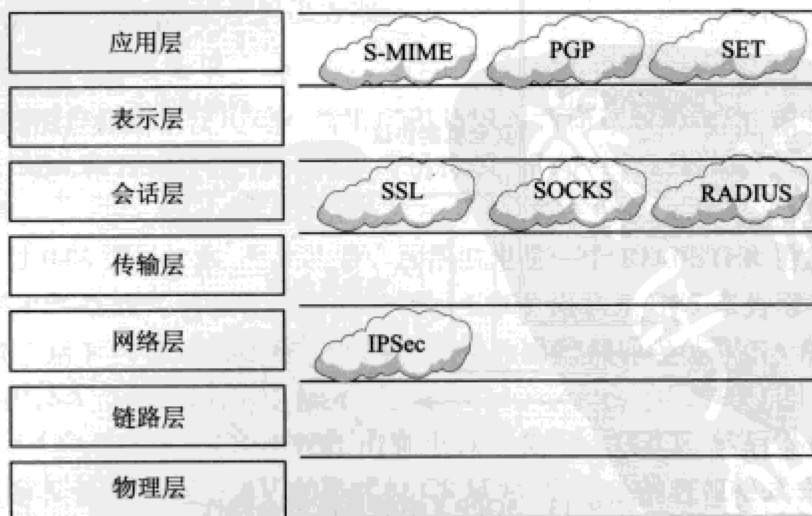


图 9.12 不同 OSI 层的安全协议(实例)

逐链路保护的意思是:连接(路径)是由通信链路组成的,如果每一个链路所传输的东西都受到了某种保护(如加密),那么整个连接就是可靠的。这种方式的缺点是,如果业务发生路由错误,则链路上传送的内容就可能暴露,而终端用户不

一定能知道这一点。

在 OSI 高层应用的安全机制一般就是端到端安全。在这种情况下，数据在达到终点之前一直受到保护（如加密）。传输的数据虽然受到了很好的保护，但黑客仍可能进行业务分析：可以发现诸如数据的发送者和接收者，传输何时进行，传输的频率如何等信息。如果要实现全网的安全解决方案，我们必须把链路级和端到端的安全机制联合起来。每个链路的加密保证了无法对路由信息进行分析，而端到端的加密减少了网络中各种节点上存在不加密的数据所带来的威胁。

在某些情况如蜂窝网络中，为了控制对蜂窝网络的接入，需要进行链路层的鉴权。在 3G 网络中，接入级的安全过程负责接入网内链路级的加密和完整性保护。在 CN 内以及在和其他网络的连接中，可以使用包括前面 9.3 节讨论的方法在内的各种方法。在 3GPP 系统中，IMS 是应用层安全机制的一个重要而又特殊的情况。在讨论一般的应用层安全机制之前，下一节我们先看一下 9.4.1 节所讲述的 IMS 安全。

9.4.1　IMS 安全

IMS（IP 多媒体核心网子系统）安全是 3GPP R5 的一个主要部分。IMS 是建立在 UMTS PS 域顶层的全应用层系统，但其设计独立于下层接入技术。因此 IMS 的安全不能单独由 UMTS R99 安全特性提供。6.4 节对 IMS 做了全面的描述。本节将进一步介绍 IMS 的安全特性，更多细节请参阅 3GPP TS 33.203。

图 9.13 示出了 R5 IMS 所有的安全特性。

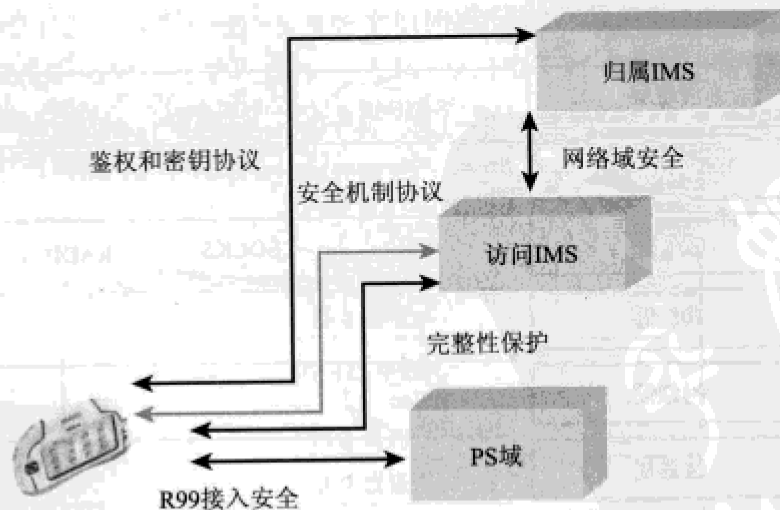


图 9.13　3GPP 5 中的 IMS 安全特性

UA（用户代理）接入 IMS 时首先在 PS 域建立一个 PDP（分组数据协议）报文。这一步骤利用了 UMTS 接入安全特性，即在 UE 和 PS 域之间相互鉴权以及 UE 和 PNC 之间的完整性保护和加密。通过 GPRS GGSN（网关节点），UA 就可以和 IMS 节点相联系，并且通过 SIP 信令的方式实现。在 IMS 中的第一次连接称为 P-CSCF（代理人呼

叫会话控制功能)。通过 P-CSCF,UA 就可以注册到归属 IMS。同时,UA 与归属 IMS 通过永久共享的主密码相互鉴权。并协议出用以保护后续 SIP 消息的临时密钥。

拜访 IMS 和归属 IMS 之间的 SIP 业务由网络域安全机制来保护。其中的 SA 并不特别针对 UA。

为了保护后续的 SIP 信令,接下来 UA 和 P-CSCF 将以安全的方式协商安全机制中所有的参数,如加密算法。然后开始 UA 和 P-CSCF 之间的所有第一跳 SIP 信令的完整性保护过程,其保护基于鉴权过程中确定的临时密钥。

所有这些特性的目的很大程度上都类似于 CS 域和 PS 域的接入安全:保护网络以防止欺诈接入,保护 IMS 网络之间的通信和 UA 以防止主动或被动的攻击。

总的来说,IMS 安全体系依靠三个主要组成部分。

(1)一个在 UE 和 HSS 之间的永久性安全文本,在用户端通过抗篡改终端里的 ISIM 安全模块得到,在网络端通过 HSS 的安全数据库得到。ISIM 和 HSS 都有 IMS 用户的识别码和相应的主密钥,它是实现 AKA 的基础。

(2)一个在终端设备和 P-CSCF 之间的临时安全文本,包括 IPSec ESP SA 和这些 SA 与 IMS 用户之间的链接。安全文本在第一跳(从 UE 到 P-CSCF 或反过来)时用来单独的给每个 SIP 消息鉴权。

(3)在不同网络节点之间的所有控制平面业务(SIP 和其他协议)都使用 9.3.3 节所述机制进行保护。相关的安全文本不针对具体用户。

以下小节将进一步介绍各种 IMS 安全机制。有两个 SIP 过程对 SIP 自身以及 IMS 安全都非常重要:用于注册的 REGISTER 和用于会话建立的 INVITE。我们围绕这两点基本功能来介绍 IMS 的安全解决方案。

9.4.1.1 鉴权与密钥协议

IMS 是按用户订制来使用的。当用户和 IMS 运营商达成协议后,用户就有了同时一个存储在 ISIM 和 HSS 中的 IMS 私有身份标识,还有一个 128bit 长的加密的主钥存储在 IMPI 内。

用户使用 IMS 服务之前,先要注册。这需要发送一个 REGISTER 消息到 P-CSCF,P-CSCF 把该 REGISTER 请求转发到 I-CSCF,I-CSCF 再联系 HSS 来为用户分配一个合适的 S-CSCF。所有这些通信以及后续网元之间的通信都通过使用 SA 的网络域安全方法得到保护,SA 与特定用户无关。

选择出 S-CSCF 之后,REGISTER 消息也就转发到 S-CSCF,然后 S-CSCF 从 HSS 出获得 AV(鉴权矢量),这些 AV 的格式与 CS 域和 PS 域中的鉴权格式一样。接着,S-CSCF 获取第一个 AV 并通过 I-CSCF 发送三四个参数(不包括 *XRES* 和可能的 *CK*)到 P-CSCF。P-CSCF 提取出 *IK*,把 *RAND* 和 *AUTN* 转发到 UE。用于装载所有这些信息的 SIP 消息为 401UNAUTHORISED,这样,从 SIP 的观点来看,第一次注册请求就已经失败了。

不过,UE 端的 ISIM 现在可以检验 *AUTN* 的有效性,如果检验通过,则计算 *RES* 和

IK。参数 *RES* 包含在一个新的 REGISTER 请求中,该 REGISTER 请求由 *IK* 进行完整性保护。完整性的保护通过 IPSec 的 ESP 协议实现。

新的 REGISTER 首先到达 PCSCF,再(经过 ICSCF)转发到 S-CSCF,S-CSCF 把 *XRES* 和 *RES* 进行比较。如果这两者匹配,向 UE 发回一个 OK 消息。

AKA 过程现在已经完成,最后结果如下。

- UE 和 P-CSCF 共享 IPSec ESP SA,IPSec ESP SA 可用来保护所有后续的通信。
- 用户在 S-CSCF 和 HSS 中的状态已经从"未注册"变成"已注册"。

S-CSCF 总是在初始注册时发起 AKA。重新注册可能跳过鉴权环节,这取决于对 S-CSCF 的选择。S-CSCF 也可以随时强制 UE 重新注册,因此,S-CSCF 如果需要就可以对 UE 鉴权。

纯粹的 SIP 是一个 IETF 协议,3GPP IMS 需要在其上建立自己的扩展。这样的扩展之一是对相互 AKA 使用 3GPP 的 AKA。有一个专门的 RFC(3310)讨论这个问题,它是 HTTP Digest(RFC2617)的扩展。

9.4.1.2　安全模式的建立

用安全机制保护一个通信信道的时候,关键在保护开始的时候。

- 使用哪些机制?
- 何时开始对每个方向进行保护?
- 需要激活哪些参数(如密钥或 SA)?

无论对于何种安全机制,阻止其运行显然是最明显的攻击:除非你把它关了,否则再强的机制也是无用的。这种攻击以及其他类似的攻击可以通过中间人攻击方式实现。

RFC3329(用于会话初始协议的安全机制)专门用于对 SIP 安全机制和参数进行安全协商。其基本思想是,首先在客户和服务器之间以未保护的方式交换安全功能列表,启动保护时再核实机制选择的有效性。该消息流示于图 9.14 中。

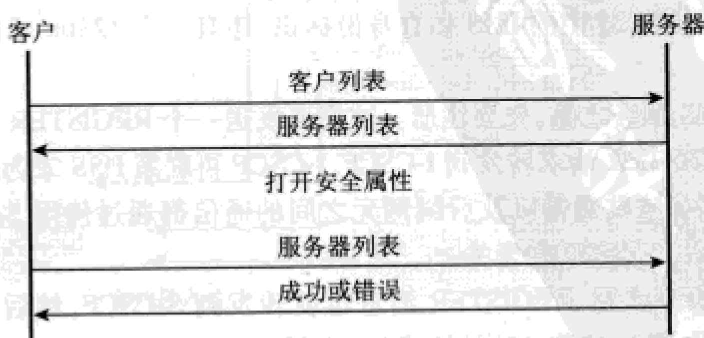


图 9.14　安全协议消息流

9.4.1.3　使用 IPSec ESP 进行第一跳保护

互鉴权不足以保证对合法用户的所有计费都能进行,因此需要对每个单独的 SIP 信令消息进行鉴权。用于建立会话的 INVITE 消息尤其必要。

完整性保护(或消息鉴权)是通过9.3.3节介绍的IPSec ESP协议实现的。采用IP层保护机制有一些补充的要求。鉴权消息的识别在ESP的情况下即为IP地址。另一方面,与IMS信令相关的计费是基于IMS身份识别的,它只有在SIP层才可见。因此SIP层的标识必须和IP地址绑定,尤其是IMPI。这个问题在P-CSCF中通过逐个校验消息来解决,SIP层用于完整性保护的IP地址在IMPI中也是允许的。IP地址和IMPI之间的链接最初由AKA建立(和ESP SA同时建立)。

9.4.2 应用层安全机制实例

在应用层,S-MIME和PGP都是常见安全机制。S-MIME对因特网MIME消息增加了数字签名和加密的安全协议。该协议最初是由RSA数据安全公司基于3-DES加密和X.509数字证书开发出来的。S-MIME使用RSA公开密钥加密方法进行加密,采用Diffie-Hellman系统进行密钥管理,采用加密哈希算法-1(SHA-1)进行数据完整性保护。

PGP(Pretty Good Privacy)是由Philip Zimmermann设计的,最初用于实现电子邮件安全的免费软件。它通过使用加密和数字签名来提供邮件的保密和鉴权。PGP最值得一提的是其分布式的密钥管理方法。这里没有密钥证书CA(认证中心),取而代之的是每个用户生成并发布自己的公钥。用户对自己的公钥签名,由此建立了一个相互连接的PGP用户团体。这种机制的优点是不需要每个用户都必须信任的CA。每个用户在一个称为"公钥环"的文件中拥有一个已经签名的公钥的集合。PGP最弱的链路是密钥撤回。如果某个人的私有密钥被盗,就必须发送密钥撤回认证。不幸的是,无法保证所有相关的使用者都能及时收到这个密钥撤回通知,这些使用者所用的公钥对应于被盗的私钥。

9.4.3 会话层安全

在OSI协议栈的会话层,可以看到SSL(安全套接层)和TLS(传输层安全)。SSL最初是由Netscape通信公司开发的,用于在因特网会话层的两个通信应用之间提供隐私性和可靠性。SSL使用公钥加密以在客户机和服务器端交换会话密钥。这个会话密钥用于加密HTTP事务(前缀为"http:\\")。每个事务使用不同的会话密钥,即使有人解密了某个事务,会话仍然是安全的(只有一个事务暴露)。

TLS是从SSL发展而来的IETF标准(RFC 2246)。它有一个针对无线环境优化了的修改版是本WTLS(无线传输层安全),用来保护WAP会话的安全。

9.4.4 AAA安全机制

在RFC2138中描述的RADIUS(远程验证拨入服务)用于在NAS(网络接入服务器)和共享鉴权服务器间传输鉴权、授权和配置信息(如图9.15所示)。RADIUS提供

了一种能让多个拨号 NAS 设备共享公共鉴权数据库的方法。它最初是由 Livingstom 公司开发并用于其 NAS 产品的 Portmaster 话路，此后开始普及。



图 9.15　RADIUS 协议数据流

NAS 使用客户端－服务器模型管理用户连接。NAS 作为 RADIUS 的一个客户，负责把用户信息发送给指定的 RADIUS 服务器。RADIUS 服务器负责接收用户连接请求、用户鉴权，并把所有客户必需的用于给用户提供服务的配置信息（服务类型如 SLIP、PPP、登录 ID、用于传输服务的登录用户的 ID 值）发送给客户。

IETF 的 AAA（授权、鉴权和计费）工作组已经开发出一个新的协议称为“Diameter”，它将在 3GPP R5 中用于 S-CSCF 和 HSS 之间的 Cx 接口，并可能逐步取代 RADIUS 而作为主要的 AAA 机制。

9.5　合法监听

安全的一个重要目标是采用一种特定的方式对信息进行加密，使得只有正确的接收者才能获得。到目前为止，本章已经给出了一些机制以说明 3G 网络是这样做的。

另一方面，许多国家的政府和法律对加密进行了限制，因此限制了网络所能提供的安全级别。除此之外，当地的规定也可能会要求政府机构能够以某种方式获得敏感信息并能监测用户，也就是说，无论是 CS 域还是 PS 域，政府机构可以监听电话或监测数据业务。GSM 在现有系统的顶层增加了这种功能。随着 3G 网络的出现，设计者从一开始就已经考虑了这种要求。

总的说来，合法监听由三个部分组成：监听设备/功能、裁绝设备和截获的信息（见图 9.16）。监听设备或监听功能搜集表 9.1 和表 9.2 所列的内容，再根据当地的要求决定要哪些不要哪些。这种过滤的功能由当地的裁决设备进行，这样，给出的信息就都是当地规定所要求的信息。这些过滤后的信息就是“截获的信息”。关于合法监听的详情可以查阅 3GPP TSs 33.106、33.107 和 33.108。

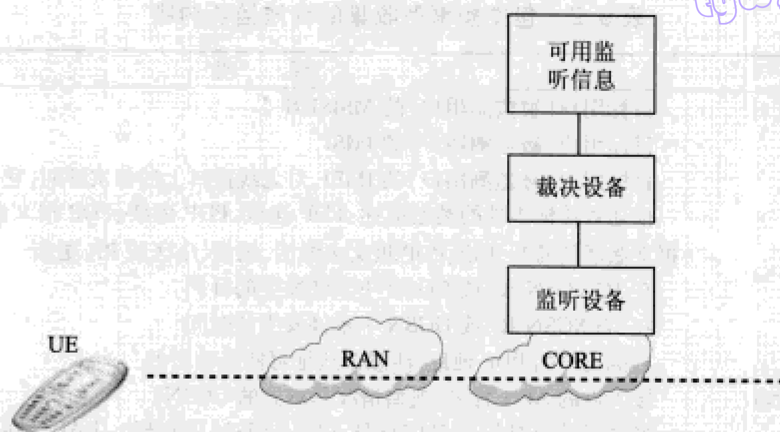


图 9.16 合法监听示意图

除了表 9.1 和表 9.2 所列出的内容外，还有一些与用户位置相关的规定。比如有些国家要求未来的系统在紧急呼叫时能显示出 50m 精度范围内的用户位置。这样的精度不能靠一般的 MM 方法来实现，为此 3G 网络中包含了一个专门的“定位系统”，以达到所需的精度。本书第 8 章已做过介绍。

表 9.1 电路交换事务收集的合法监听内容

内 容	说 明
观察的 MSISDN	目标用户(被监测用户)的目标标识 MSISDN
观察的 IMSI	目标用户(被监测用户)的目标标识 IMSI
观察的 IMEI	目标用户(被监测用户)的目标标识 IMEI，应对无线接口的每次呼叫都进行检查
事件类型	要传输的事件描述：建立，应答，补充业务，切换，释放，短信，位置更新，用户控制输入
事件日期	3G MSC 中事件生成日期
事件时间	3G MSC 中事件生成时间
被叫号码	数位转换、智能网号码转换前的被叫号码
连接号	应答方的号码
对方地址	对 MOC(手机主叫)来说是对方的电话号码，对于 MTC(手机被叫)则是主叫号码
呼叫方向	被监测用户是呼出还是呼入
关联号	用于关联每一个呼叫和截获信息的唯一号码
网元标识码	相关网元(如 MSC)的唯一标识
位置信息	作出记录的当时，在 3G MSC 中表示的服务区标识或位置区标识
基本业务	有关电信业务和承载业务的信息
补充业务	目标使用的补充服务(如 CF、CW、ECT)
呼叫转移号码	在 CF 的转移号码
呼叫释放原因	目标呼叫的释放原因
短信发起者	短信是移动台主叫、移动台被叫或者未定义
短信	短信内容，包括随短信一起发送的头部
重定向号码	引起呼叫转移到目标的号码。如果没有就不提供
SCI	3G MSC 从 ME 接收到的与呼叫无关的 SCI

表 9.2　包交换事务收集的合法监听内容

内　容	说　明
观察的 MSISDN	目标用户（被监测用户）的 MSISDN
观察的 IMSI	目标用户（被监测用户）的 IMSI
观察的 IMEI	目标用户（被监测用户）的 IMEI，对无线接口上的每次呼叫，它都要被校验
事件类型	描述要传输事件的类型描述：PDP 连线、PDP 离线、PDP 报文激活、随着 PDP 报文激活的监听开始、PDP 报文去激活、短信、小区或 RA 更新
事件日期	在 3G SGSN 和/或 GGSN 中事件发生的日期
事件时间	在 3G SGSN 和/或 GGSN 中事件发生的时间
PDP 地址	目标用户的 PDP 地址，注意该地址可能是动态的
接入点名字（APN）	接入点的 APN 名字（典型情况是对方的 GGSN）
位置信息	事件记录当时的位置信息是 SAI（业务区识别码），RAI（路由区识别码）或 LAI（位置区识别码）
先前位置信息	在 RA 更新之前的用户位置信息
PDP 类型	使用的 PDP 类型（如 PPP，IP 或 X.25）
关联号	关联通信内容和与监听相关信息的唯一号码
短信	短信内容、短信头，头也包含短信中心地址
网元标识码	相关网元（如 SGSN）的唯一标识码
连线失败原因	连线到目标用户失败的原因
失败的报文激活原因	目标用户报文激活失败的原因
IA	被观察的监听区域
会话发起者	PDP 报文激活、去激活或更改请求的发起者，即网络或 UE
主叫	指示短信是移动台主叫还是移动台被叫
去激活/终止原因	PDP 报文终止的原因
QoS	指示和 PDP 报文相关的 QoS
服务系统地址	关于服务系统的信息，如 SSGSN 序号或 SSGSN 地址

第三部分

第 10 章 UMTS 协议

前面几章以子网和网元为主对 UMTS 网络进行了介绍。网元之间的功能主要是按对网元的系统级管理功能划分的。同时还介绍了网元之间的各种接口。

本章则以 UMTS 网络中的接口为重点关注系统的协议。UMTS 协议用于在系统接口之间以协调的方式控制网络功能的执行。

10.1 节～10.6 节先介绍适用于 UMTS 网络(即 UTRAN 和 CN)的协议。由于 IMSC IP 多媒体系统接入独立的特性,IMS 网络和服务协议将在 10.7 节中单独介绍。

10.1 3GPP 协议参考结构

由于协议规范工作分配在 3GPP 技术组织的不同工作组中进行,因此自然就形成了不同组为各自负责的协议开发出相应的协议参考结构。其结果产生了三种主要范围,各有其自身的协议参考模型。

在介绍贯穿本章的 UMTS 所有网络协议的组合模型之前,我们先对上述三个参考模型逐一进行介绍。从这些协议中可以看到一些主要的协议结构概念,它对我们导出组合协议结构很有帮助。

10.1.1 无线接口协议参考模型

UTRAN 无线接口是基于 WCDMA 无线技术的,它和 2G 的无线接入技术有一些本质的区别。无线接口协议主要控制不同种类和不同来源的业务流的复用。为了保证对复用的有效控制,对任务进行了严格的分层。这就产生了图 10.1 所示的三层协议参考模型。

这些层根据它们在结构中所处的位置,简单地命名为无线接口 L1 层、L2 层和 L3 层。虽然在设计中使用了著名的 OSI 的分层原则,但是这三层并不能看成是 OSI 模型中最低的三层。这些层有明确的功能划分,层与层之间有详细的接口定义,因此也可以命名如下。

- L1——无线物理层。
- L2——无线链路层。
- L3——无线网络层。

如图 10.1 所示,物理层以 WCDMA 传输信道集的方式提供它的服务。因此物理层负责第一次复用功能:把传输信道的数据映射到物理信道,或进行相反的映射。传输信道到物理信道的映射关系见第 4 章。

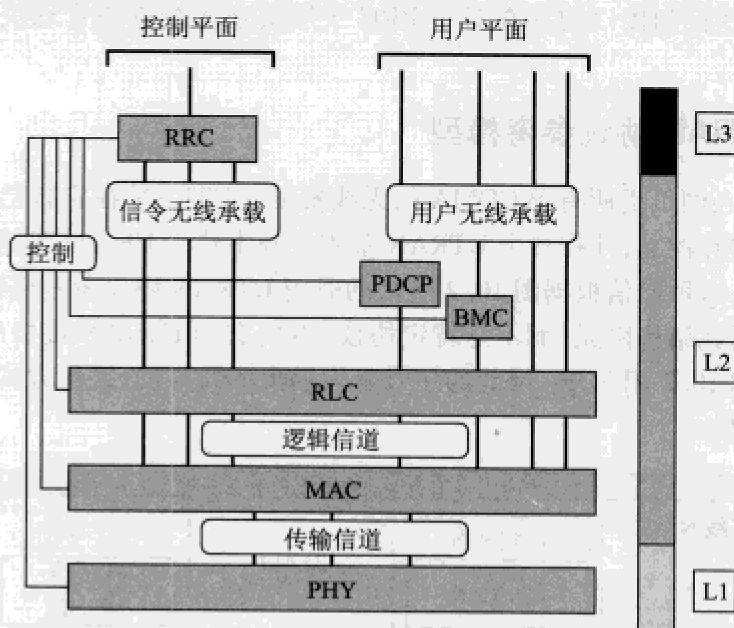


图 10.1 无线接口协议参考模型

无线链路层是另一个复用层,主要负责 WCDMA 无线接口容量的动态共享。与 L1 层传输信道的多样性不同,无线链路层使高层看到的只是一些无线承载,不同的业务借助这些承载通过无线链路进行传输。UTRAN 无线承载是 UMTS 系统承载体系的一部分(见第 1 章)。

MAC(媒体访问控制)子层控制传输块容量的使用,确保 UTRAN 端所做的容量分配能及时在无线接口两端执行。RLC(无线链路控制)子层再对 MAC 子层提供的逻辑信道添加常规的链路层功能。针对无线传输的特点,RLC 子层还增加了一些特有的功能。

RLC 服务能满足 L3 控制协议(信令)的需要,但是对于特定领域的用户数据,还需要附加的会聚协议才能完成全部的无线承载服务。CS 域数据(如编码转换的语音数据)不需要会聚功能,但 PS 域必须要有附加的会聚子层。PDCP(分组数据会聚协议)子层使 UMTS 无线接口能够传输 IP 数据名。另一个会聚协议(BMC,广播/多播控制)用于消息广播和多播,主要任务是调度发送到 UE 的小区广播消息。

控制信令和用户数据的分离是在协议工程中长期应用的另一个主要的设计原则。根据这个原则,用于控制功能的协议将成为系统级控制平面的一部分,而承载用户数据的协议则属于用户平面。

L3 层的控制平面协议是 RRC(无线资源控制)协议。如图 10.1 所示,在 UTRAN

和 UE 侧，RRC 协议实体同所有其他协议实体一样都存在接口。一旦由 RRC 控制的协议实体位于其他的 UTRAN 网元中，就需要使用标准的协议来支持这种控制机制。在其他情况下，控制接口集成在一个单独的 UE 或 UTRAN 网元的内部，所以没有严格的标准化，但是这些控制接口的存在对于 RRC 子层实现无线资源管理决定的任务是非常重要的。

10.1.2　UTRAN 协议参考模型

UTRAN 接入网负责所有 WCDMA 的无线资源。UTRAN 在它自己的网元内进行无线资源的管理和控制，并在整个 UTRAN 基础设施中建立 UE 和 CN 进行通信所需的无线接入承载。这种通信根据图 10.2 所示的通用 UTRAN 协议参考模型进行结构化。通用的意思是说其结构网元（而不是特定协议）对所有的 UTRAN 接口（Iu、Iub 和 Iur）都是相同的。图 10.2 用 3GPP 规范的序号来表示具体的协议，这种方式也强调了公共协议结构的思想。

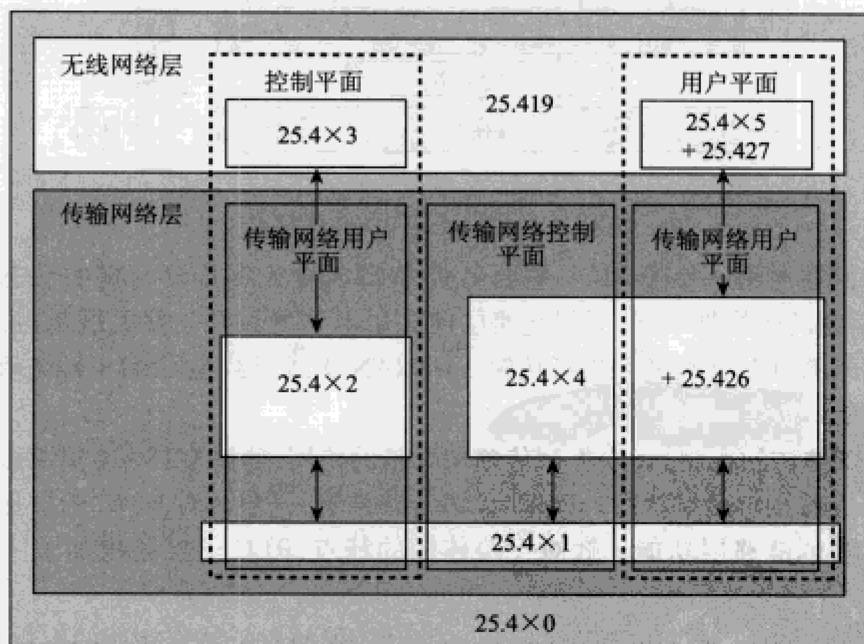


图 10.2　通用 UTRAN 协议参考模型

UTRAN 协议体系的主要元素是层和平面。UTRAN 设计采用通用的原则将协议栈分成两个主要部分。所有的底层协议一起组成了 UTRAN 的"传输网络层"。这里的，"传输"和 OSI 中的意义基本相同，即它覆盖了这样一组协议，允许非邻接的网络节点通过多种可能不同的子网进行通信。另一个实际考虑是从现有的协议中选择用于传输层的协议，而不是为 UTRAN 设计专用的协议。

对应于无线接口协议模型,位于传输网络层之上的其他协议集称为"无线网络层"。这些是专为 UMTS 系统设计的,用于各种 UTRAN 接口的无线接入承载的管理和使用。

图 10.2 也示出了控制平面协议和用户平面协议的划分。这种设计思想已经在无线接口协议的设计中进行了讨论,其思想已用于 UTRAN 所有接口的设计中。传输网络层协议的选择是非常审慎的,所选择的协议要能够以最好的方式支持控制平面和用户平面所需要的各种属性。对于控制平面来讲,协议选择的依据主要是能够保证可靠性;而对于用户平面,则从另一方面考虑,其依据是传输网络所能提供的 QoS(服务质量)。无线网络层的控制协议是为了满足无线和承载控制的要求而专门设计的。UTRAN 无线网络层控制协议通常称为"UTRAN AP(应用部分)协议"。另一方面,无线网络层内负责用户数据帧的用户层协议通常称为"UTRAN 帧协议"。

UTRAN AP 和帧协议一起组成了 UMTS 接入层,覆盖所有与所选无线接入技术相关的通信问题。对于一般的 UMTS 无线接入承载,非接入层协议则用于在 UE 和 CN 之间直接传输信令和用户数据帧的透明流。非接入层的这些功能是通过把高层负载封装到 UTRAN 协议消息中来实现的。

UTRAN 控制平面协议是按照客户端—服务器的原则来设计的。在 Iu 接口,UTRAN 扮演无线接入服务器的角色,CN 作为客户端向 UTRAN 请求接入服务。同样在 Iub 接口,BS 作为服务器,它的 CRNC 作为客户端。在某种程度上,Iur 接口也类似,DRNC 作为服务器提供具有远程 BS 可控性的 SRNC。在基于客户端—服务器的协议设计中,服务器协议实体的行为是根据它从客户端接收到请求时所做的动作确定的。另一方面,客户端在什么情况下产生这样的请求是可变的。

Holma 和 Tlskala 在其著作 *WCDMA for UMTS*(2004)中对 UTRAN 协议结构进行了更详细的讨论。

10.1.3 CN 协议参考模型

CN 由支持网络特性和终端用户业务的网元组成。提供的支持包括用户位置信息的管理、网络特性和业务的控制以及信令和用户生成信息的传输(交换和传递)等功能。

在 CN 中,3GPP R99 的协议结构是从 GSM/GRPS 系统演进而来的,因此可以分为五个主要的协议组。

- UE 和 CN 之间的非接入层协议。
- 业务和归属网络的网络控制信令协议。
- 分组数据骨干网络协议。
- 传输网络控制协议。
- 业务控制协议。

由于是从 GSM/GPRS 继承的,因而这些协议有不同的背景和来源规范。

一个典型的例子就是,UMTS CN 终止来自 UE 的非接入层协议。非接入层协议很

明显受 GMS/GPRS 背景的影响。这些在著名的"鼻祖"GSM 04.08 的演进版本 3GPP TS 24.008 中有明显的体现。非接入层协议的设计目标是使 UMTS 系统和 GSM/GPRS 系统保持兼容，以共享同一个核心网和支持双模用户设备。

UMTS 非接入层协议栈如图 10.3 所示。所有这些协议由信令连接承载，信令连接是在初始接入和信令连接建立阶段，在 UE 和 CN 之间建立的。在 PS 域和 CS 域，非接入层协议有两个不同的子层。较低的子层负责 MM(移动性管理)，在 CS 域中称为 MM 协议，在 PS 域中，由于它处理 GRPS MM，所以称为 GMM 协议，与具体服务有关的 CM(通信管理)协议在这个通用子层之上运行。CM 协议和它们的控制功能如下。

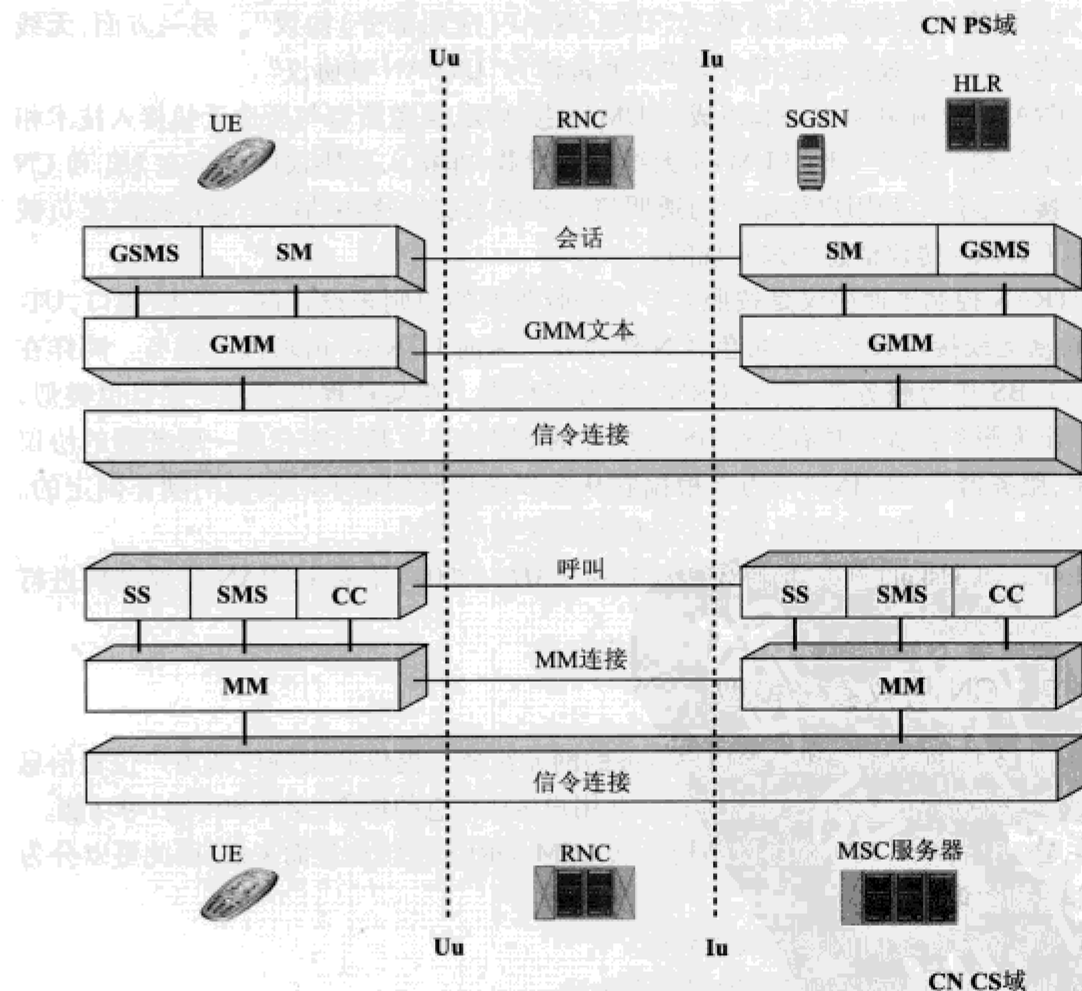


图 10.3　UMTS 非接入层协议

- SM(会话管理)协议，用于控制在 CN PS 域内分组数据传输的 PDP 文本(会话)的建立和释放。
- CC(呼叫控制)协议，控制 CN CS 域内电路交换呼叫的建立和释放。

- SS(补充服务)协议,控制各种与呼叫有关和呼叫无关的补充服务的激活和去激活。
- GSMS/SMS(短消息服务)协议,控制来自 UE 或到达 UE 的短消息的传输。

服务网络和归属网络之间的网络控制信令使用了 MAP(移动应用部分)协议集,该协议集最初设计来控制 GSM CS 业务。由于 GRPS 子系统引入了 PS 业务,这就需要扩展 MAP 协议来支持 GPRS 的节点和归属网络的节点间的接口。在图 6.4 示出的 3G 核心网接口中,下面这些由 3G 版本的 MAP 协议来控制。

- 起源于 GSM 系统的 C、D、E、F 和 G 接口。
- 起源于 GPRS 系统的 Gc、Gr、Gf 和 Gs 接口。

这意味着正常情况下,SGSN 和 GGSN 都必须使用 MAP 协议来实现控制平面功能。

MAP 协议采取了面向事务的通信策略。每个事务(如在 HLR 用户位置的注册)在 CN 节点之间会被当成对话来执行。这种通信结构是由底层的事务能力应用部分(TCAP)子层来为 MAP 子层创建的。TCAP 进一步使用基于 SS7 信令的传输网络作为跨网络运营商的信令骨干网。

CN PS 域用于分组数据传输的协议组也被 GRPS 骨干网所采用。它遵循了在 GPRS 规范制定之前就已完全建立的网络间协议范例和 IP 协议组。实际上只需要增加一个特定的 GPRS 的协议就可以了。GTP(GPRS 隧道协议)在 Gn 和 Gp 接口中控制跨 PS 域骨干网的通信(见图 6.4)。

GTP 协议也可以分为两个子协议:用于 SGSN 和 GGSN 之间信令控制的 GTP-C;由 GGSN 扩展来的,从 Iu 接口到 UTRAN 侧的用户平面协议 GTP-U。这种在 RNC(而不是 SGSN)上中止的 GTP-U 通信与最初 GPRS 规范不同。

任何 UMTS 网络都必须和外部的电信网和数据通信网进行互连。这种互通涉及整个传输网,在这种情况下的电路交换业务是指国际的 PSTN/ISDN 骨干网,而对分组交换业务它经常是指另一个 IP 骨干网。因此传输网络边界的协议必须和传输网络骨干网的协议一致。在电话网中,往往选择 ISUP(ISDN 用户部分协议)或者 BICC(独立呼叫控制协议)。相应地,在 IP 数据网里,IPv4 或 IPv6 将用于网络互连。

在归属网络和拜访网络中,UMTS 核心网都应能为用户提供增值服务。因此业务控制协议 CAMEL 的 CAP(应用部分协议)要从 GSM 结构中保留下来。这在第 2 章网络演进中已经进行了讨论。CAP 是另一个基于事务的协议,因此像上面讨论的 MAP 协议一样,它可以使用 TCAP 业务和国际 SS7 信令骨干网。

10.2 UMTS 协议交互结构

10.1 节所述的大量不同种类的 UMTS 系统协议或许有些容易让人产生混淆。由于在协议选择和设计中必须考虑继承性,所以 UMTS 系统协议不可能是一个统一和一

致的协议集合。本节将详细介绍 UMTS 网络的组合协议结构模型，以便在这一章的后面对每个协议进行更进一步的讨论。

通过对无线接口、UTRAN 和 CN 协议的讨论，我们已经熟悉了下面两个协议设计原则。

- 通过分层使(通用的)传输部分和(UMTS 相关的)移动网络部分分离。
- 通过分层使网络控制部分和用户数据部分分离。

在进一步讲述之前，先来了解一下建立网络范围协议体系时，需要考虑的另外两个基本设计问题。

- 协议互通。
- 协议终止。

协议互通涉及同一层但扩展在多个网元上的协议，这些协议集合决定系统范围内公共功能的(分布式)执行。这些公共系统级功能的例子如无线接入承载的建立和位置更新。前一个例子需要从 UE 到 CN 网元的互通以及 UTRAN 内来自 RRC 协议和 AP 协议的协同工作。对于位置更新，互通的"协议链"包括 MM 协议(UE 和 CN 间)和 CN 节点间的 MAP 协议。协议设计者把这样一个分布行为的"链"叫作一个(系统)过程。

协议互通也经常设计为上面提到的、对客户端—服务器模型的扩展。一旦在网络的一端触发了事件，首先发现这个外部事件的协议实体就成为客户端，并通过向它的服务器请求服务来开始程序。在一个 UMTS 网络中，服务器很少能单独满足这样的请求，而是作为另一个客户向另一个服务器发出其他请求，此过程直到那些服务器(通常在与触发事件发生相反的网终端点)达到不能进一步委派任何任务时才停止发送请求，但服务器仍必须服从它们自身的命令。在无线接入承载建立中，这个过程最先是由 CN 网元发起的，最终由 BS 和 UE 通过建立它们之间的连接来完成的。位置更新过程是由 UE 发起的，最终是由 HLR 把位置信息记录到数据库中。

第11章还有更多完整的例子来描述 UMTS 系统级的过程。但是在本章中，我们对 UMTS 协议采用分层观点设计时，其关键是对层内互通协议的设计。

协议终止现在就可以看成是上述协议链的终点。在协议终止的网元中，系统功能或算法就是数据或命令的源或目的地。对于上面提到的位置更新例子中的 MM 协议，终止点就是 UE 和 HLR。有时谈论的终止只涉及一个单独的协议，此时的终止点就是这个协议的两端。因此从系统级协议体系来看，一组互通协议的终止点更为重要。

本章剩余部分把 UMTS 协议集分成三个不同的分层子系统协议来讲述。每一部分自身可以看成一个逻辑网络。这种分解并不严格遵循 3GPP 规范的体系，而是从网络级和面向协议的观点来分解的，其主要原则是分层和端到端的互通。

首先，UMTS 协议模型在水平方向上进行分层。每层的协议在多个接口上使用，共同执行上面所讲的协议互通。

图 10.4 表示了三个不同的层。

- 传输网络层。
- 无线网络层。
- 系统网络层。

在这种划分中,传输网络层负责为所有 UMTS 网元提供通用的传输服务,使它们能够在所有网络接口间进行通信。通过在无线网络层和系统网络层使用 UMTS 系统特有的协议,UMTS 系统的功能就可以分布到网络的各个单元中。无线网络层协议保证了 UE 和 CN 之间与所有无线接入承载有关的互通。系统网络层协议从 UE 扩展到 UMTS CN 的传输网边缘,保证了与 UMTS 通信服务相关的互通。

所有三层都可以分为控制平面和用户平面,它们给图 10.4 所示的 UMTS 协议模型增加了另一个维。所有涉及控制的协议都属于控制平面,所有涉及用户数据传输的协议都属于用户平面。对于无线网络层和系统网络层,用户平面和控制平面的区别是很明显的。但是对于传输网络层,许多协议则同时用于控制平面和数据平面。为了优化性能,某些协议专用于传输控制数据而另一些则专用于传输用户数据。

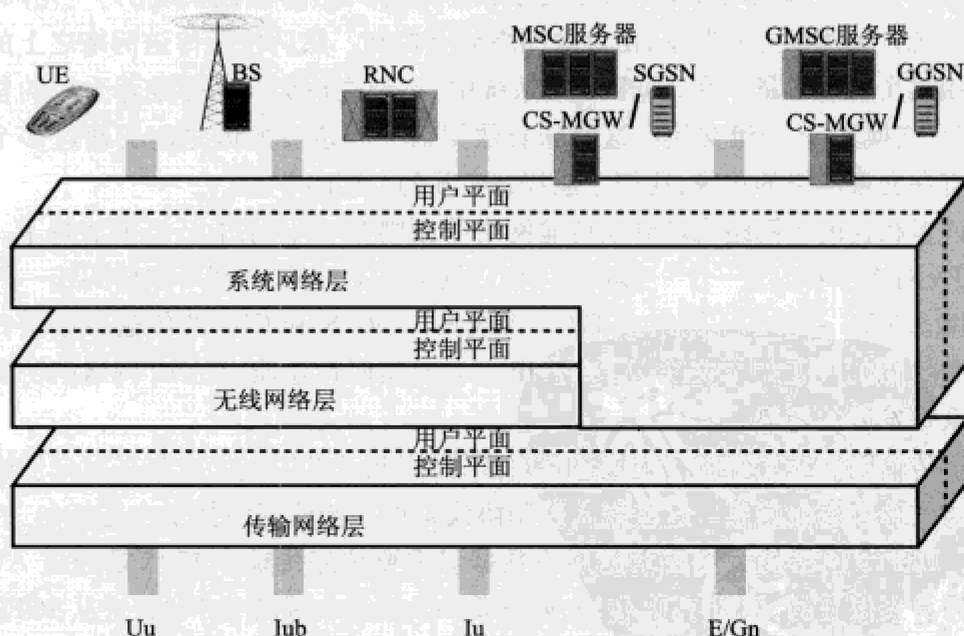


图 10.4 UMTS 协议互通体系

不同 UMTS 系统接口的控制平面协议彼此间相互作用,保证了对通信资源和服务的系统级控制。使用同样的方式,用户平面协议彼此间相互作用,保证用户数据的端到端传输。

根据用户业务的不同特性,分出了两个不同的系统域。在 CS 域中,用户平面的容量在整个服务(如电话呼叫)期间分配到电路中;在 PS 域,用户平面的容量分配到数据分组中。这两种域的区别也表现在传输网络协议的选择和系统网络协议的设计上,因

此本章在必要时对其分别进行阐述。

有了这样的划分，三个不同的协议子系统就可以随时由于技术的原因而进行升级。实际上，3GPP版本5在引入其他传输网络协议和新的IMS时就体现出了这种演进。

10.3 传输网络协议

控制平面和用户平面的通信容量在理论上可以是物理分离的，但这样做会浪费网络中的无线和有线资源。因此尽可能多地为用户平面和控制平面设计了通用目的的传输服务协议，作为各自的一个子系统，称为“传输网络”。

顾名思义，UMTS传输网络实际是UMTS网络中的一个网络。但只要再仔细研究一下传输网络技术，就可以发现它不仅仅是一个网络，而是由多个子网络组成的。对UMTS系统来说，可以看成是一个单独的UMTS逻辑传输网络。

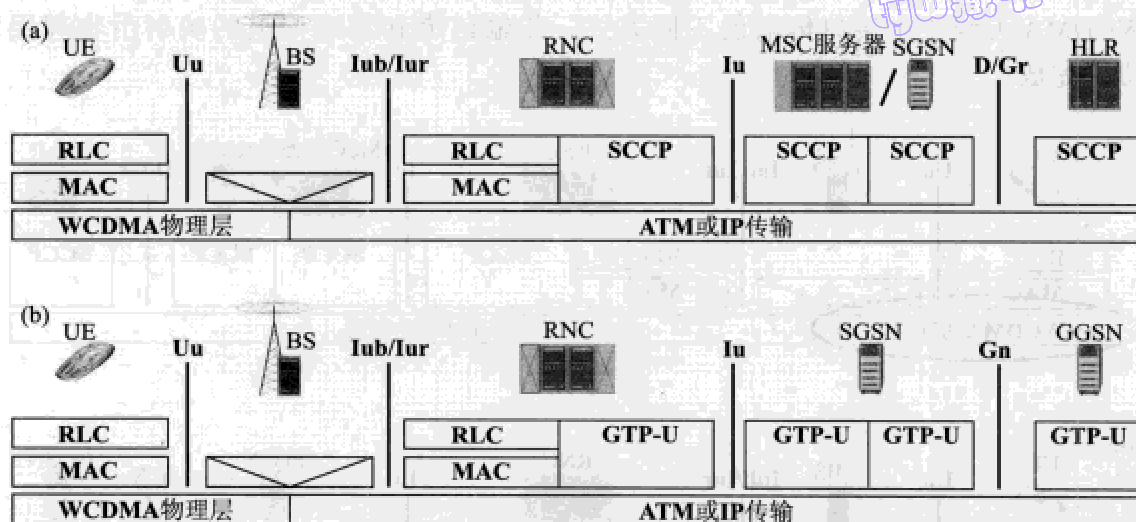
比特的物理传输是通过基于数字传输技术的(蜂窝)传输网实现的。(光)骨干线的容量以统计复用的方式共享，由传输网络节点控制。然后位于传送网络之上的二级网络利用这个传送容量。在3GPP R99系统中，对于这种交换网络推荐采用的技术是ATM信元交换和IP分组交换。这意味着数据信元到达目的地之前要通过多个交换机。只有在交换网络的边缘，我们才能找到实际的UMTS网元。

把许多相连的子网组成端到端传输网络的原则在IP体系中已经很清楚了。同样地，UMTS网络可看成是一个“互联的网络”，只是它不遵循IP网络那样的统一协议结构。相反，UMTS系统的不同组成部分(无线接口、RAN和CN)的传输服务是各自独立设计和优化的。正如下文所说，基于IP并具有实时传输能力的IP网络的协调传输网络体系是发展的趋势。

由于传输网络本身提供了交换和路由能力，因此可以用嵌入控制平面来创建传输网络电路或分布路由信息。这些嵌入控制协议是根据传输网络技术来选择的，这里不再详述。UMTS网络的关键要求是用户数据组需要按序传输。ATM是通过ATM信元交换自身来保证的，但对于IP传输，就需要一个设计良好的IP网络，这从3GPP标准来看并不是一个问题，因为UMTS传输网络是一个特别针对运营商的专用网络，不会被其他许多公共IP传输所共享。

10.3.1 传输网络协议结构

传输网络组成了UMTS协议结构的最底层，提供了在UMTS所有网络接口中对控制和用户业务进行传输和路由的功能。图10.5表示了最重要的传输网络配置:信令传输网络和分组传输网络。



(a)传输网络中的控制平面协议;(b)传输网络中的用户平面协议(仅在 PS 域)

图 10.5 3GPP R99 传输网络协议

物理层通过控制物理媒体来传输控制信令和数据业务。UMTS 无线接口的物理层是基于第 4 章所述的 WCDMA 无线技术而设计的。物理层协议的功能是为高层提供一组 WCDMA 传输信道。

3GPP 对 ATM 传输和 IP 传输网络的地面接口都有规定。在 R99 中,ATM 及其适配层(AAL2/AAL5)是最流行的传输选择,而 IP 传输只对 Iu-PS 做了规定,是用户平面的唯一选择和控制平面的选项。从 R5 开始,ATM 传输和 IP 传输对用户平面和控制平面的 UTRAN 接口来说都是同样的有效选项。

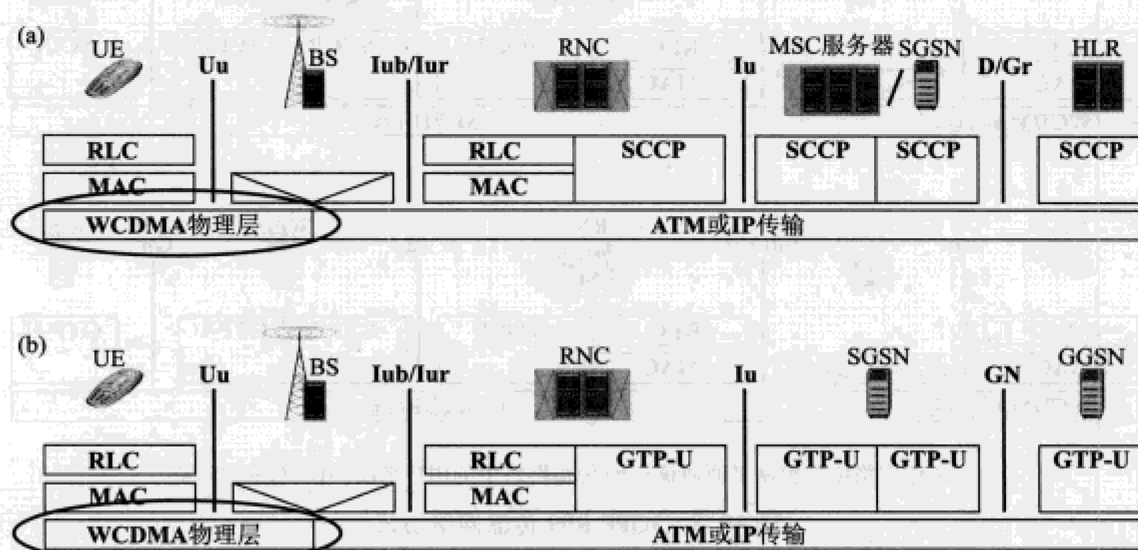
支持 ATM 和 IP 传输所需的物理层传输媒质以及合适链路层是开放选择的,目的是为了不限制运营商对传输网技术的使用。但是需要指出的是 3GPP 对 IP 传输有一个默认的假设,即认为 UTRAN 是专用于运营商自己业务的私有网络。这有助于解决安全和 QoS 问题,否则就要在 IP 网络协议和技术选择中进行详细的规定。作为运营商 UTRAN 传输的私有网络,需要有一个设计良好且具有充足额外业务的 IP 网络。

图 10.5 给出了一个简化的用于 UTRAN 无线接口的传输网络协议栈。由于 UTRAN 内部协议结构和功能的划分,MAC 和 RLC 协议将终止于 RNC,因此需要在 Iur/Iub 接口上传输 MAC/RLC 帧。用于承载 MAC/RLC 帧的帧协议并没有在图 10.5 中示出,但是在 10.4.2.2 节将会讨论到。这些帧协议既可以在 ATM 传输顶层运行,也可以在 IP 传输的顶层运行。在 UTRAN 中,由 SRNC 负责 WCDMA 传输信道级中 UE 与无线接口相关的操作,而 BS 实际上只维持 WCDMA 物理信道。

10.3.2 在 Uu 接口中的 WCDMA 物理层

物理层协议控制 WCDMA 物理信道在 Uu 接口的使用,如图 10.6 所示。物理层协议以 WCDMA 传输信道的形式向高层提供服务。传输信道定义了数据在

WCDMA 无线空中接口传输的不同方式。传输信道和物理信道的映射由物理层协议完成。



(a)传输网中的控制平面协议;(b)传输网络的用户平面协议(只在 PS 域)

图 10.6　Uu 接口中的无线传输

物理层根据带宽提供按需服务,这意味着传输信道能够支持可变速率传输。作为最底层,物理层还负责 WCDMA 帧级的复用。为管理这种复用,物理层协议对传输信道所使用的传输格式进行控制。传输格式定义了传输块在传输信道上每个传输间隔内的传输格式。传输块集合是通过 MAC 协议实体组成的物理层 SDU 的集合,其中 MAC 协议实体使用物理层的服务。传输时间间隔决定了物理层以怎样的频率接收 MAC 数据。传输格式属性列在表 10.1 中。

表 10.1　WCDMA-FDD* 传输格式属性

动态属性	传输块大小 传输块集合大小
半静态属性	传输时间间隔 差错保护方法:类型、编码速率、速率匹配 CRC 大小

* 表示频分双工。

物理层对来自不同传输信道的传输块进行复用。为了维持 WCDMA 无线传输的帧同步,物理层也执行把传输块分割成无线帧的操作。此外,物理层还进行信道编码、交织和速率匹配。这些操作都是在无线帧映射到不同的物理信道之前完成的。

值得注意的是,与 GSM 无线系统的物理层协议不同的是 WCDMA 系统在物理信道不进行加密。

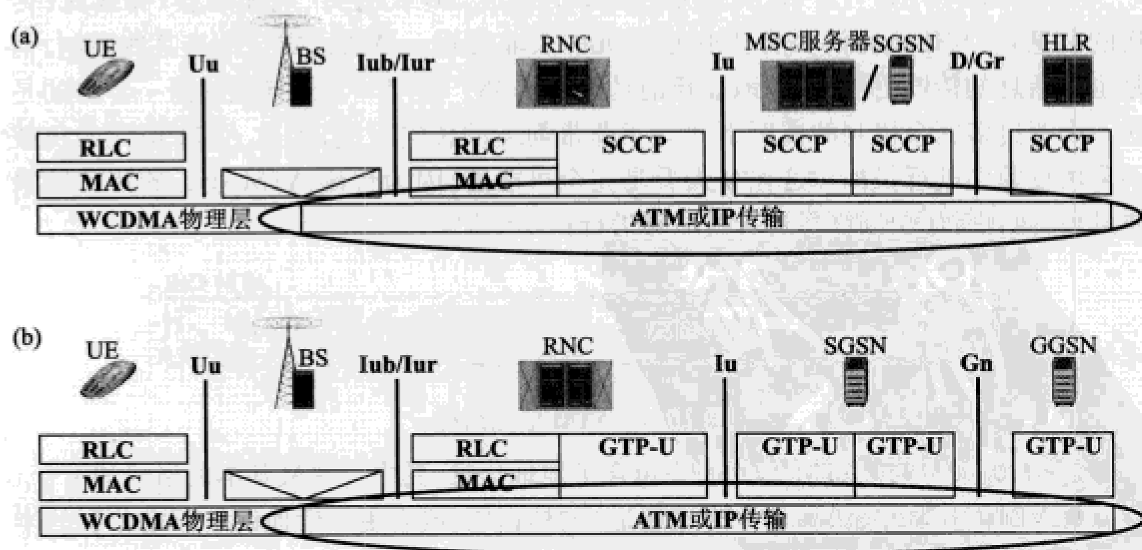
物理层协议也把 CRC 校验和(0、8、12、16 或 24bit)加入到要在空中接口传输的传输块中。在接收侧,物理层把传输块和根据 CRC 校验得到的错误指示比特一起传输给高层。

WCDMA 物理层提供的服务在 3GPP 规范 TS 25.302 中有详细描述,而 3GPP 规范 TS 25.211 ~ 25.215 包含了所有物理层协议的详细描述。Holma 和 Toskala 在 2004 年对物理层进行了更详细的阐述。

10.3.3 其他接口中的骨干网

同无线接口不同,UMTS 有线接口的传输网络协议不是专用于 UMTS 传输的。相反,它是 3GPP 从现有协议集中选择出来的。和所有传输网协议一样,选择传输网络协议的焦点在于对不同终端用户(确切说是不同 UMTS 承载)的业务进行复用,并顾及 QoS 特性。

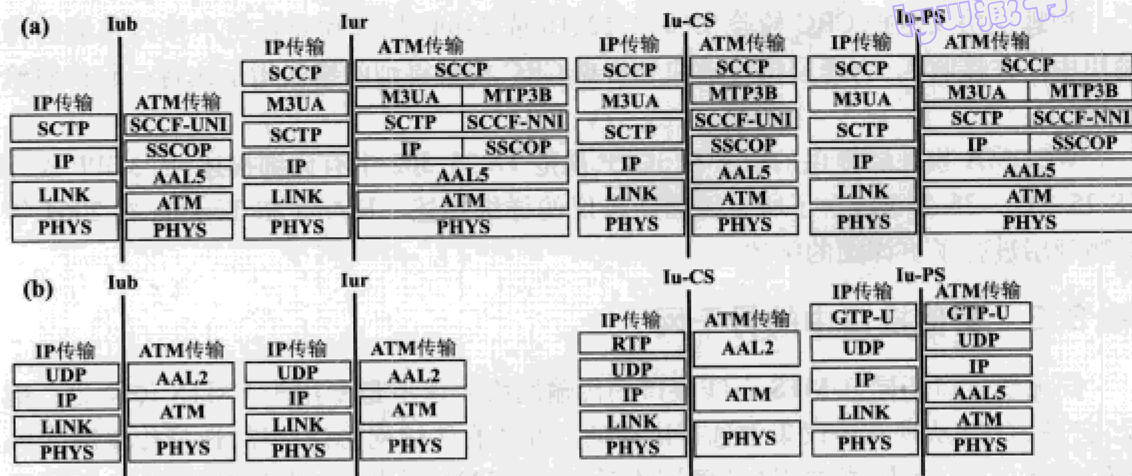
再考虑到一些不可避免的标准化政策因素,UMTS 由此选择了两个主要的协议组:一个来源于宽带通信的 ATM 协议族,另一个来源于因特网的 IP 协议族。在 3GPP R99 中,ATM 是 UTRAN 侧主要的传输网络技术,同样地,IP 是核心网中分组域的主要技术。在核心网的电路域中,传输网仍旧采用基于时隙的 PCM 中继网。在 3GPP R5 中,包括 Iu-CS 接口上的语音发送在内的所有接口中,ATM 和 IP 传输都是同等有效的选择。如图 10.7 所示。



(a)传输网中控制平面;(b)传输网络的用户平面协议(只在 PS 域)

图 10.7 在其他接口中的传输网

在这两种情况下,在 UMTS 中使用 ATM 或 IP 都需要一些适应和会聚协议以在通用目的协议的顶端运行 UMTS 标准传输协议。图 10.8 给出了 3GPP R5 为不同接口规定的完整协议栈。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议

图 10.8 ATM 和 IP 传输协议栈

10.3.3.1 ATM 传输

ATM 的基本思想是把要传输的信息流分割成小的分组,加上地址标签后通过物理传输路径传输。接收端收集接收到的分组,然后根据分组的内容组成最初的信息流。这些包含传输信息的分组叫 ATM 信元。

如图 10.9 所示,一个 ATM 信元由两部分组成,5B 长的头(地址信息)和载荷(传送的信息)。与传统协议和消息相比,信元的头非常短。虽然这样会带来某些限制,但是也使信息的传输更加有效:地址开销是 5/(5+48) ~9.5%。这样做的另一个目的是在不需要过多冗余机制的情况下建立了非常简洁的传输系统,因此 ATM 信元的负载不采用校验和进行保护。这在今天看是完全可能的,因为传输 ATM 业务的传输网络质量高,而且所使用的终端自身就能够进行错误保护。



图 10.9 ATM 信元结构

如图 10.10 所示,ATM 信元的头包含了地址信息,其中一些最基本的格式如下:

- VPI(虚通道标识):是 VP(虚通道)的标识码,或者更一般地说是恒定分配的半永久连接的标识码。
- VCI(虚通路标识):是 VC(虚通路)的标识码。由于一个 VP 包含成百上千个通路,因此这个域比较长(比如,多媒体应用可能同时需要几个 VCI,每个多媒体单元分配一个 VC)。
- PT(负载类型):指示 48B 的负载所承载的是用户数据还是控制数据。
- CLP(信元丢失优先级):指示 ATM 信元的重要性。如果 CLP=1(低优先级),

系统可以在必要的时候丢弃该信元。

- HEC(头错误控制):对 ATM 信元头部进行错误保护的原因是信元头部出错要比负载出错危害更大,例如头部信息出错可能会使信元传输到错误的地址。所使用的纠错机制可以发现头部的所有错误,并可以纠正一个错误。

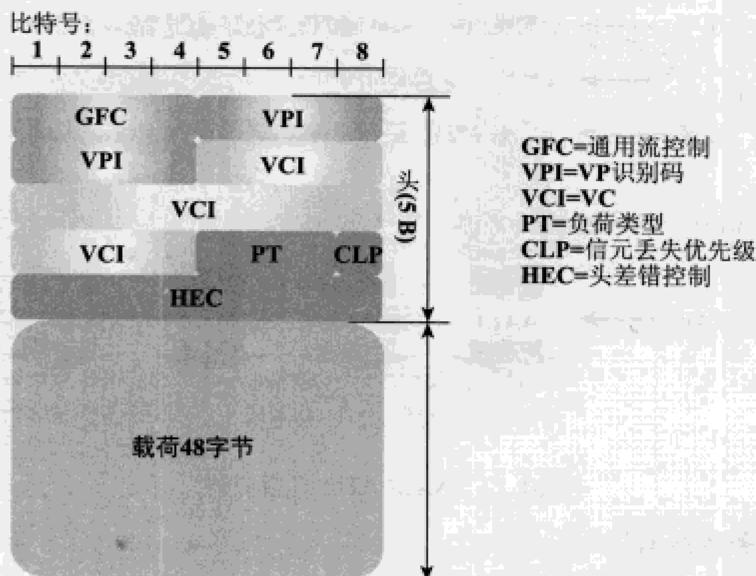


图 10.10 ATM 信元头结构

图 10.11 示出了 ATM 的传输路径。一条 ATM 传输路径由几个 VP 组成,一条 VP 又包含很多 VC。

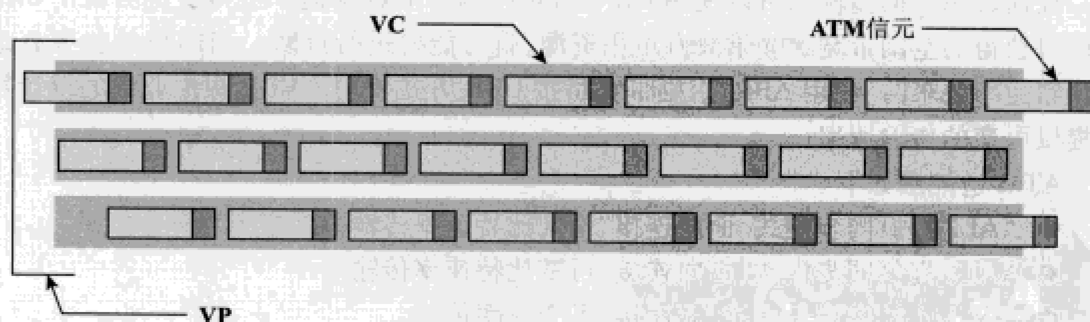


图 10.11 VP 和 VC 关系

VP 是一个半永久连接,能够同时处理许多虚连接 VC。实际的数据是经过 VP 在 ATM 信元中传输的。从 UMTS 系统的观点来看,ATM 传输路径是指 BS 和 RNC 之间的路径。如果要进行环路传输,传输路径要包含许多虚路径(每个基站一个),并且 VC 中的 VP 在每一次呼叫建立时都要建立。虚通道的带宽取决于所使用的承载业务。

这样的 ATM 层包含简单的传输媒体,理论上讲也非常适合传输。但在实际应用中,ATM 层要对更高的协议层和更低的物理层进行适应。ITU-T 已经定义了采用

AAL 的"ATM 业务等级"。最初的想法是让 ATM 从 A 到 D 等级的业务分别与 1 到 4 个 AAL 相对应。随着时间的推移,这种想法已经不存在了,如图 10.12 所示。

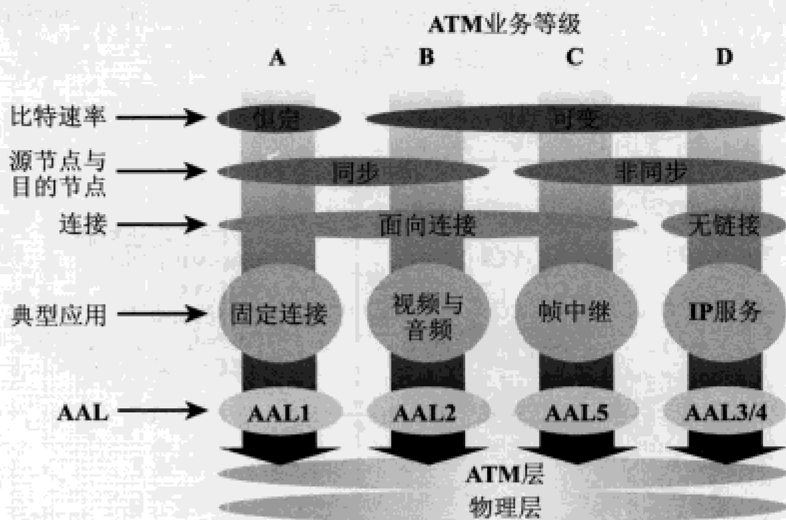


图 10.12 AAL(ATM 自适应层)

ATM 的业务等级有以下几项。

- CBR(固定比特速率业务)。
- UBR(未定义比特速率业务)。
- ABR(可用比特速率业务)。
- VBR(可变速率比特速率业务)。

任何透明数据传输都可以使用 CBR,且可根据峰值数据速率进行资源分配。UBR 使用可获得的空闲带宽。如果没有可用资源,就可能要进行排队。当用户的业务有最小比特速率要求时,使用 ABR,否则带宽将按 UBR 方式使用。VBR 根据业务的统计特性提供可变的传输速率。

ATM 适配层如下。

- AAL1 提供同步模式、面向连接、恒定比特速率传输。
- AAL2 提供同步模式、面向连接、可变比特速率传输。
- AAL3/4 提供异步模式、无连接、可变速率传输。
- AAL5 提供异步模式、面向连接、可变比特速率传输。

如图 10.13 所示,AAL 分为两个子层:会聚子层 CS 和分割与重组子层 SAR。CS 使 AAL 与高层协议适配。SAR 在发送端把要传输的负荷数据进行分割,在接收端接收负载数据并把它们还原成最初的形式。CS 子层还可以分成更小的实体。

从 UMTS 传输网络的观点来看,AAL2 和 AAL5 是最佳的选择。AAL2 对电路交换的用户平面连接来说是很合适的,而 AAL5 则适合于控制协议交换。有关 UTRAN 协议接口中 AAL 的变化详见表 10.2。

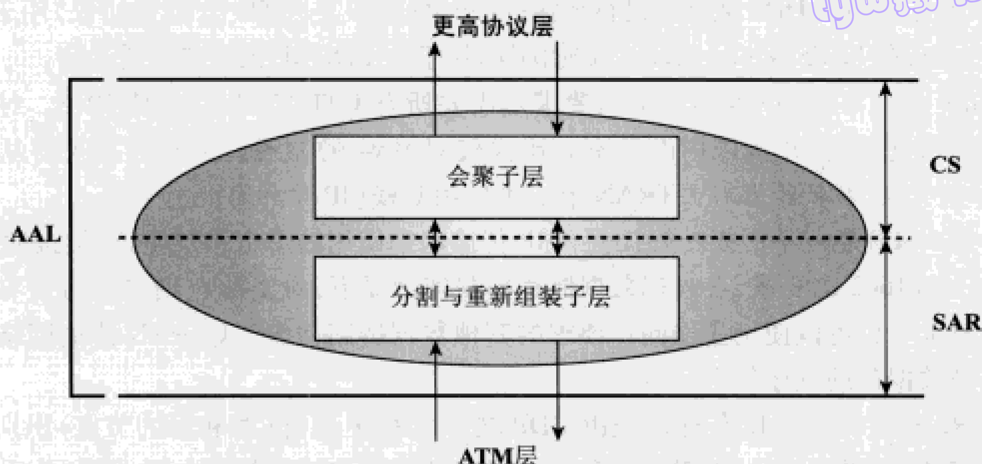


图 10.13 AAL 通用结构

表 10.2 适用于 UTRAN 接口处的 ATM 适应层

AAL5	Iu:CS C 层,PS C/U 层,传输网络内部的 C 层
	Iur:C 层,传输网络内部的 C 层
	Iub:C 层,传输网络内部的 C 层
AAL2	Iu:CS U 层
	Iur:U 层
	Iub:U 层

注:C 层 = 控制平面;U 层 = 用户平面。

在 UTRAN 中,ATM 适配层 AAL5 用于传输所有控制协议和 Iu 接口的 PS 域用户数据。相反地,除了 PS 域 Iu 接口的用户数据,其他所有接口用户数据的传输都可以使用 AAL2。

图 10.8 给出了在不同 UTRAN 接口中的 AAL 协议栈子层,在此将不做详细描述。选择这些会聚协议的关键就是,在 R99 系统 PS 域所有控制平面协议中,会聚有两种方式可供选择:它们是 ITU-T 为了在 AAL5 上传输信令而制定的会聚协议集以及 IP-over-AAL5。除此之外,在 Iu 接口处 PS 域的用户会聚已经是 R99 的一部分,并且是基于 IP 的 UDP(用户数据报协议)产生的。在 3GPP R5 中,这就导致了在所有的 UTRAN 和 CN 接口中对基于 IP 的传输有更广泛的应用,接下来将对此进行阐述。

10.3.3.2 IP 传输

在 3GPP R99 标准制定过程结束时,基于 IP 的传输受到了更大的关注。IP 互连技术将作为 UMTS 网络未来发展的共用传输方式,为了给 IP 互连技术的全面利用创造一个基础,在所有 UTRAN 接口中对信令和用户数据传输进行的 IP 选项的研究是非常必要的。

尽管使用 3GPP R5,用户数据还可以通过使用 IP 协议栈在所有的 UTRAN 接口进行传输(如图 10.8 所示)。用于数据传输的 IP 栈的公共部分是 UDP/IP:在 Iub 和 Iur 接口

上,无线帧作为明码 UDP 数据包进行传输;在 Iu-PS 接口上,GTP-U(隧道协议)用于装载用户数据包;在 Iu-CS 接口上,RTP(实时协议)用于在 UDP/IP 顶层装载语音帧。

3GPP 规范对 UTRAN 传输网的要求是需要所有 UTRAN 节点支持 IPv6。对 IPv4 的支持是可选择的,并且该标准并不妨碍仅仅对 IPv4 的实现。然而为了支持从 IPv4 到 IPv6 的升级,我们推荐在 UTRAN 节点中使用双栈(IPv4 和 IPv6)。

尽管 3GPP 规范不需要托管任何在 IP 传输网中使用的单链路层协议,但按照 IETF RFC1661 和 1662 的要求,在高速数据链路控制帧情况下,对支持点到点的协议有一个最小的要求。也可以使用遵循同样要求的其他数据链路协议。UTRAN 传输网络的主要要求是数据包的顺序传送。

UTRAN 接口中的 IP 传输承载由 UDP 端口号和 IP 地址(源和目的节点)识别。出于 QoS 考虑,根据 IETF RFC2474,每一个在 UTRAN 传输网中的 IP 节点必须支持 DSCP(差分服务码点)。

为了保持 UMTS 信令的 IP 传输以及 ATM 传输之间的协调,这两个栈应该提供相同的传输服务。因此就确定了要对这两个使用信令连接控制部分 SCCP 协议实体的栈进行“表面化”,而该协议实体总可以提供相应的信令传输服务(形成的协议栈结构见图 10.8)。

因为 UMTS CN 基于 GSM/GPRS 网络子系统,因此信令传输协议是从 GSM/GPRS 继承下来的。3GPP R99 的实现仍包括基于共用信道 SS7 的协议栈。虽然使用了 3GPP R4/5,但也可通过在 ATM 或 IP 顶端运行 CN 信令协议,使 CN 信令传输解决方案和 UTRAN 传输网一致。

在 SS7 信令网的情况下,SCCP 协议运行在 MTP3(Message Transfer Part Layer 3)协议顶层,MTP3 负责在信令点之间路由信令消息。MTP 路由是基于信令码并且只能够在一个单一的 SPC 寻址空间之内路由信令消息。该寻址空间通过一个网络运营商来进行管理。为了使跨网络边缘进行路由成为可能,需要使用 SCCP 协议。SCCP 采用全局名寻址,比如,对于访问网络中的 VLR 可使用 HLR 的全局名在用户归属网内找到 HLR。

通过使用两个会聚协议,实现了 SCCP 协议在 IP 协议栈上的适配。IETF SIGTRAN 工作组进行了相关的标准化工作。这些协议和相应的 IETF 文档如下。

- SCTP(流控制传输协议),RFC 2960。
- M3UA(MTP3 用户适配层)(因特网草案)。

这两个子层的目的是使 SCCP 层位于常规的 MTP3 业务之上,MTP3 业务在通信信令网络的使用已经有二十多年了。

SCTP 是被假定在 IPv4 或 IPv6 网络上运行的。更重要的是,假定其工作在性能良好的实际 IP 网络上。这在实际中意味着其下层存在多个路由网络以避免单一节点失效的问题。SCTP 也考虑了用多个 IP 地址/端口的多归属端点来增加可靠性。而且,为了决定数据路径的 MTP 大小,它提供了 MTPMTU 的发现功能,这也避免了 IP 级的碎片。

SCTP 协议的目的是提供可靠健壮的信令传输承载。为了实现这个目的，SCTP 提供适当的拥塞控制，用消息丢失时的快速重传来加强可靠性。它还提供了额外的安全防护机制来防止盲攻击，可用于加强不同运营商的网络进行连接时的安全性。

M3UA 协议用来支持 SCCP 信令，以使 SCCP 底层的接口不需要进行修改就可以直接使用。当运行在 IP 层之上时，M3UA 协议需要管理 SCTP 流的使用并且其性能和 SS7 中相对应的 MTP3b 协议能匹配。M3UA 协议提供从 SS7 地址到 IP 地址的映射，同时提供失败跳过支持和端点间的负载分担。

M3UA 协议有两个体系模型：信令网关到 IP 信令点 IPSP，IPSP 到 IPSP。一般认为 IPSP 到 IPSP 模型是最简单和最实用的模型。

10.3.4 UMTS 传输网络协议

上述运行于传输骨干网（ATM 或 IP）之上的协议提供了 UMTS 节点之间信令寻址和路由，并允许将不同用户的业务复用到共用的传输网容量中。WCDMA 物理层自身有一定的复用能力，此外，传输网中物理层之上的层也有多路复用的任务。

10.3.4.1 Uu 接口的传输网络协议

负责在 Uu 接口传输电路域和分组域所有控制信令和用户数据的传输网络协议如下。

- MAC 协议。
- RLC 协议。

这两个协议共同组成了传输网络的无线链路层。

10.3.4.1.1 MAC 协议

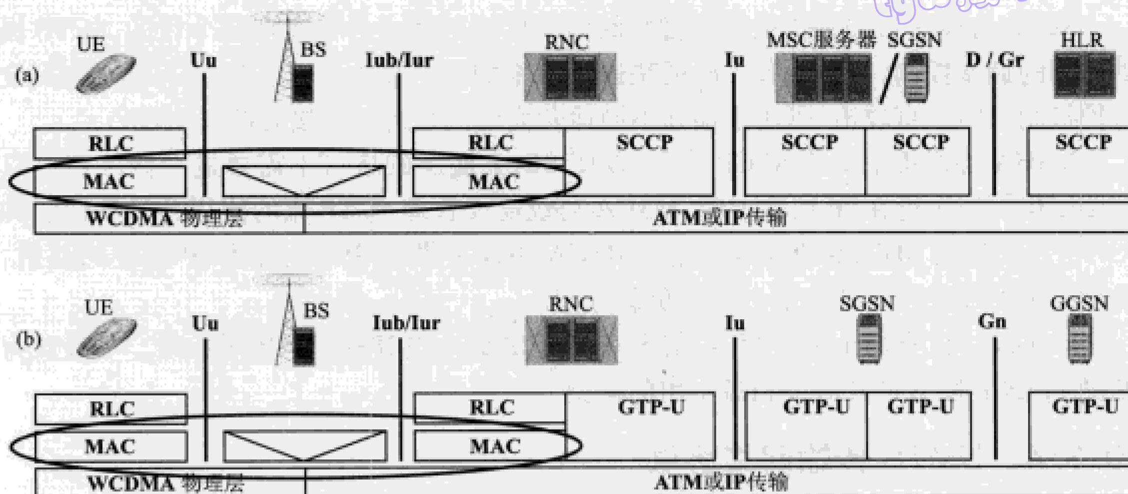
MAC 协议在 UE、BS 和 RNC 实体处激活（如图 10.14 所示）。MAC 是 L2 协议，作为公共传输网络的一部分，它为控制平面和用户平面提供服务。MAC 协议在设计之初就已经考虑了 PS 和 CS 业务以及信令传输，这是和 2G 无线分组协议的主要区别。2G 无线分组协议可以看成是在一般的 CS（时隙）2G 无线载波上叠加了针对分组数据的协议。

MAC 协议以逻辑信道的方式提供服务，逻辑信道根据所传数据的类型来定义。如第 4 章所述，这些逻辑信道包含四种逻辑控制信道和两种逻辑业务信道。

MAC 协议负责对所有由物理层提供的 WCDMA 传输信道上的通信进行控制。为了能够在一组用户间共享传输信道的容量，MAC 协议以传输块为单元进行传输。提供给 MAC 的每个传输信道的传输块大小由 WCDMA 物理层传输格式集来定义。

物理层 MAC 所提供的传输信道类型可以分为三种：公共 MAC、专用 MAC 和广播 MAC。

公共 MAC 实体位于 CRNC 和 UC 之中，负责对公共和共享信道进行控制。MAC 协议能够把来自高层的 PDU 复用成在公共传输信道上传输的传输块集。在公共传输信道上根据临时标识（由 RNC 来分配）来识别 UE，临时标识可以是小区无线网络临时标识（16bit 的 C-RNTI）或 UTRAN 无线网络临时标识（32bit 的 U-RNTI）。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.14　传输网络——媒体接入控制 MAC

专用 MAC 实体属于 SRNC 和 UE,并提供对专用传输信道的控制。专用传输信道 MAC 能够通过把高层 PDU 组成传输块集来进行复用。这种情况下,属于一个集合的所有传输块必须属于一个 UE,因为传输信道是 UE 专用的,并且只有当 QoS 参数与专用信道所支持的业务相同时才能进行复用。

广播 MAC 实体在基站和 UE 中。该实体在每一个小区中只处理一个广播传输信道。

在任何传输信道初始化数据发送之前,MAC 实体都会为给定的传输信道选择一个合适的传输格式并考虑其他传输信道的数据发送要求。来自每个信道的不同传输格式组合是根据任意时刻提供的业务的瞬时比特速率和功率控制情况而建立的,不同传输格式的组合形成了图 10.15 所示的传输格式组合。

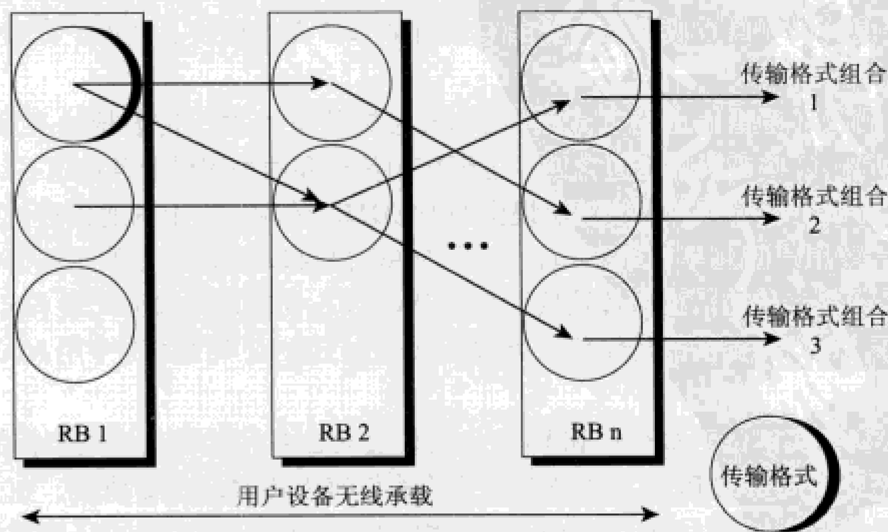


图 10.15　在 MAC 协议中的传输格式组合

由于 MAC 也是用户平面的一部分,因此它也是实时协议。MAC 要满足严格的物理层定时要求,并且 MAC 需要根据物理层指示的传输间隔来发送新的传输块集合。在每个传输间隔内,MAC 必须根据所要传输数据的特性和当时的业务状况选择最优的传输格式组合。

MAC 层提供的基本服务是在对等端 MAC 实体间进行数据传输。值得注意的是,从高层来看,该服务是不需要任何确认和分割的。

虽然交换配置的命令是从 RRC 层发出的,但是公共信道、专用信道、共享信道之间的交换也是由 MAC 层来执行的。

MAC 也要收集 RRC 层使用的业务的统计信息。这些 MAC 测量由每个逻辑信道来提供,并且包括如下一些本地测量,例如缓冲区占用、均值和方差。关于每个传输信道是否过载或未满载的 MAC 状态指示和测量模式(事件触发或周期进行)也要报告给 RRC。

MAC 层执行透明模式 RLC 数据的加密。MAC SDU 在专用逻辑信道上发送(DCCH 和 DTCH)并且被映射到使用每个 UE 特有的密钥进行加密。加密使用第 9 章所述的块加密算法 KASUMI。

MAC 协议只有一种 PDU,叫作"数据 PDU",它由 MAC SDU 和 MAC 协议头组成。协议头根据要使用的传输通道来构造。在某些情况下(如 UE 只有一个 DCH 且没有任何逻辑信道复用时),MAC 协议头也可以不要。

在 3GPP R5 标准中,MAC 也支持 HSDPA(高速下行链路分组接入)。作为该扩展的一部分,引入了一个全新的高速 MAC 实体。高速 MAC 实体主要负责控制新的传输信道:HS-DSCH(高速下行共享信道),是一种存在于每一个可进行高速下行分组接入的小区的共享信道。该信道介于 UE 和 BS 之间,其两端都由高速 MAC 对等体控制。在 BS 和 SRNC 之间,高速业务是通过"专用 MAC 流"(MAC-dedicated Flow)实现的,这是 R5 中的又一扩展。从专用 MAC 来看,专用 MAC 流可视为另一种专用传输信道,和 DCH 类似。

由于 HS-DSCH 传输信道没有方向属性(它只存在于下行链路方向上),MAC 高速对等实体执行着非对称的功能。在 BS 处,高速 MAC 执行和数据传输相关的功能,比如在用户及其优先队列之间进行时间分配,优先处理和传输格式选择等。在 UE 端,高速 MAC 需要考虑数据接收,包括按照优先级以及高速 MAC PDU 的拆卸对队列中的数据进行重新排序。

为了提高数据传输的可靠性,高速 MAC 对错误的已传数据 PDU 进行快速重传。每一个高速 MAC PDU 通过相关的上行链路信令被接收机确认,根据接收到的确认信息,发射机可以启动重传。不过,无论高速 MAC 接收机何时发现错误,它并不马上丢弃接收到的错误包,而是存储到软缓冲器中,然后和重传的包进行相干合并,直到该包可以解码为止。UE 端的高速 MAC 能进行软合并,软缓冲器的容量由 RRC 层配置。

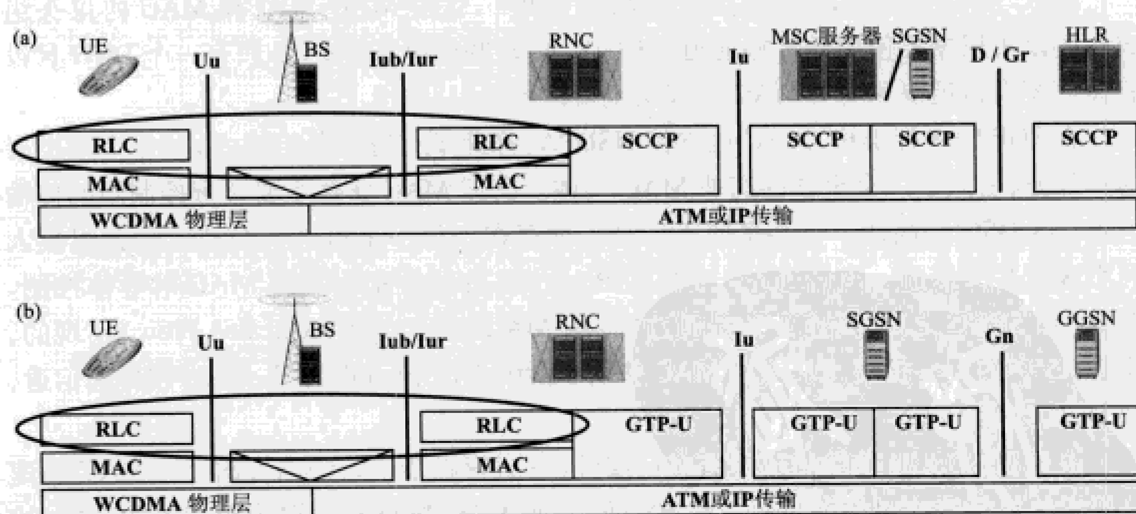
快速重传和软合并是由n信道HARQ(混合自动重复请求)功能块实现的。每个UE端的高速MAC有一个HARQ实体,BS端的高速MAC每小区有一个HARQ实体。每个实体最多有8个停止等待(stop-and-wait)信道。

BS中的高速MAC实体从专用MAC流接收数据并按照优先级重新排序。在每一个由发送物理层提供的TTI(传输时间间隔,可以只有2 ms),只可以处理从一个队列中接收到的数据。每一个队列的时序速率(如间隔时间多久能在HS-DSCH获得发送/接收的)权利取决于调度算法。因此,在BS端高速MAC和SRNC中的专用MAC之间,为了避免队列溢出需要流控制功能。流控制功能是借助HS-DSCH帧协议容量分配过程实现的。

对MAC协议的完整描述在3GPP规范TS25.321中给出,对MAC协议更详细的讨论也可以查阅Holma和Toskala的著作(2004年)。

10.3.4.1.2 无线链路控制RLC协议

RLC协议既可以在RNC中使用,也可以在UE中使用,用来完成WCDMA空中接口的一般数据链路层功能(如图10.16所示)。RLC在控制平面和用户平面可以同时被激活,也可以同时为电路交换连接和分组交换连接提供数据链路业务。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在PS域)

图10.16 传输网——RLC

RLC的运行环境依赖于所使用的平面:在用户平面由PDCP协议来使用RLC,在控制平面由RRC协议来使用RLC。RLC的底层协议是MAC,MAC以MAC SDU形式在逻辑无线信道中提供数据传输服务。由于MAC数据传输是非确认模式的,所以RLC就要对传输需要可靠性保证的高层PDU负责。而且由于MAC不能根据可使用的传输格式对大的SDU进行分割,所以要由RLC来承担这项功能。因此传输格式在RLC层是可见的,如图10.17所示。

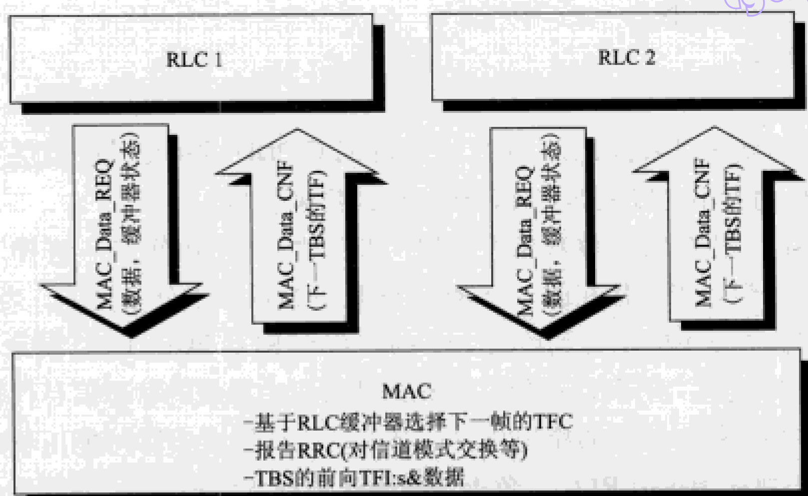


图 10.17 专用信道上 RLC 与 MAC 的通信

RLC 通过 RLC SDU 提供高层 PDU 的数据传输业务，这种业务称做为无线承载业务。RLC 定义了三种操作模式:透明模式 Tr、非确认模式 UM 和确认模式 AM。

在透明模式中，RLC 发送 SDU 时不添加任何协议信息。可以对 SDU 进行分割和重组，但这样做必须在无线承载建立时，在 RRC 层进行协商。这种模式可用于流类业务。

在非确认模式中，RLC 不保证 SDU 能可靠传输到对等端实体。这种模式可以被某些 RRC 控制过程使用，其中的确认信息是由 RRC 协议自身来处理的。

在确认模式中，RLC 可以保证能可靠传输 SDU 到对等端实体。可靠传输是通过重传的方式来保证的。如果 RLC 不能正确传输数据，发送端的用户能接收到通知。这种模式用于在专用逻辑信道传输分组交换数据。

RLC 层要执行许多功能，如下。

- 分割和重组。
- 拼接。
- 填充。
- 纠错。
- 顺序传输 SDU。
- 重复检测。
- 流控制。
- 序号校验。
- 协议错误检测和恢复。

- 暂停或继续功能。
- SDU 丢弃。
- 加密。

分割和重组是指对来自 RLC PDU 或是到 RLC PDU 的可变长度高层 PDU 进行调整。RLC PDU 的大小可以根据实际的传输格式集来调整。

当 RLC SDU 没有填充整数倍个 RLC PDU 时，将使用拼接。这样下一个 RLC SDU 的第一个分组可以连接在前一个 RLC SDU 的最后一个分组上了。当不使用拼接并且剩余的传输数据不能填充到给定大小的整数个 RLC PDU 上时，剩余的数据区域将由填充比特来填充。对于反向链路，填充比特可以由承载的状态信息代替。

RLC 的许多功能与差错的检测和纠正有关。比特错误实际可能由物理层的 CRC 校验来检测，但错误纠正由 RLC 层负责。在确认数据传输模式中，重传可以提供最有效的错误恢复。RRC 通过配置 RLC 协议来进行不同的重传方案（如选择重传、倒退 N 步或停等方案等）。

SDU 的顺序传输保证了使用确认数据传输服务的高层 PDU 的传输顺序。如果不使用顺序传输，传输顺序混乱就可能发生。

RLC 也能检测到接收到的 RLC PDU 是否重复，保证合成后的高层 PDU 仅向高层传输一次。流控制使 RLC 接收端能够控制对等端 RLC 实体发送消息的速度。

序号校验功能可用于非确认模式以保证重组 PDU 的完整性。在 RLC PDU 重组成 RLC SDU 时，通过 RLC PDU 的序列号校验提供对受损 RLC SDU 的检测，受损 RLC SDU 将会被丢弃。

协议错误检测和恢复功能可以通过执行 RLC 协议来发现和恢复错误。RLC 复位过程用于从错误的情形下恢复。对于不可恢复的错误，PLC 实体要向 RRC 层报告。

RLC 可以根据 RRC 的请求暂停或继续数据传输。

如果经过很长时间后 RLC PDU 仍没有成功发送，那么 SDU 的丢弃功能就将删除发送端缓冲区中 SDU 剩余的 RLC PDU。SDU 丢弃功能防止缓冲区溢出。RLC SDU 丢弃功能可以由其他几个操作模式替代。

RLC 层的加密用于使用确认模式和非确认模式的无线承载。加密功能用 UE 特有的密钥完成，加密算法是第 9 章所述的块加密算法 KASUMI。

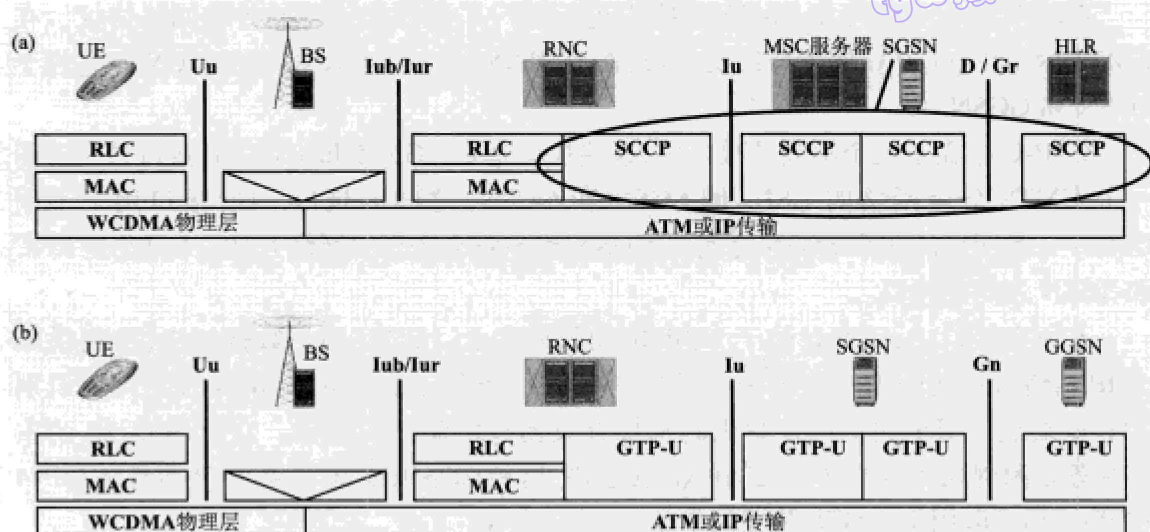
在 3GPP 规范 TS25.322 中完整地描述了 RLC 协议，如想了解更为详细的内容也可以查阅 Holma 和 Toskala 的著作（2004 年）。

10.3.4.2 其他接口中的传输网协议

10.3.4.2.1 信令传输（SCCP）

UTRAN 和 CN 接口中的共用信令传输协议是 SCCP（如图 10.18 所示）。

SCCP 是从 SS7 中继承下来的，既可以提供无连接的业务，也可提供连接的业务。



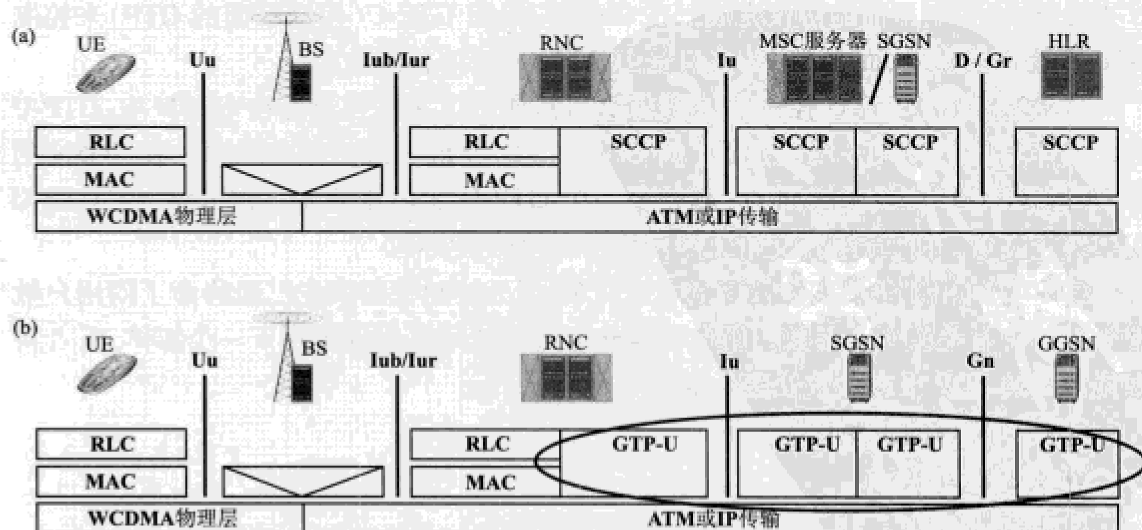
(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.18 传输网——信令传输

面向连接的业务用于支持信令承载。

10.3.4.2.2 用户数据的 IP 传输(GTP-U)

在 CN PS 域和整个 Iu 接口中,提供传输服务的主要用户平面协议为 GTP-U,用于分组数据用户平面(如图 10.19 所示)。从名字可以看到,它主要来源于 2G 的 GSM/GPRS 系统,但是协议的结构设计选择明显不同。在 2G 中,GTP-U 协议仅在 2G-GSN 网元之间使用,但是在 3G 中,它又穿过 Iu-PS 接口扩展到了 RNC。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.19 传输网络——用户平面的 GRPS 隧道协议

GTP-U是一种支持在UMTS网络中进行用户平面数据传输的传输网络协议。在UMTS网络中,GTP-U属于分组交换域,在UTRAN侧它位于RNC中,在CN侧它位于SGSN和GGSN中。

GTP-U存在于三个不同的接口中,这些接口是Gn、Gp和Iu-PS。Gn接口是属于同一个UMTS分组网络的GSN(即SGSN和GGSN)之间的接口。Gp接口用于不同UMTS分组网络的两个SGSN之间或GGSN和SGSN之间的网络互通。Iu-PS是RNC和SGSN之间的接口。

在所有接口中,GTP-U位于UDP/IP协议族之上。UDP(用户数据包协议)提供两个IP网络节点间的无连接的消息传输。UDP寻址用于在源网元和目的网元间识别GTP-U端点。UDP也提供校验机制来检查数据包传输中的错误。众所周知,IP的主要业务是源网元和目的网元之间的消息选路,这种选路则是基于网络IP地址的(IPv4和IPv6都可以用于UMTS传输网络)。

GTP-U为高层提供了无连接的数据传输业务,而且允许多协议用户数据在Iu-PS、Gn和Gp接口间使用隧道。即使分组域IP骨干网使用了不同的路由协议,封装和隧道机制也能实现用户分组数据的传输。另外,在UTRAN和GGSN间传输用户数据包的UMTS网元和协议不需要为关联用户数据包和特定的PDP报文而了解IP层寻址的差别。

由于GTP-U协议的主要目的是传输用户数据,因而特地为此进行了优化。GTP-U把从一个接口(如GGSN的Gi接口)接收到的数据标志为多个目的地(不同的UES)的数据进行复用。GTP-U从外部分组网络接收用户数据分组,解析分组的目的地址,然后将分组传送到路径的下一个节点。在GTP-U端点间建立隧道的任务已经从GTP-U去除,改由控制平面的协议完成。在Gn接口是由GTP-C(控制平面的GTP)来控制GTP-U隧道的建立,而在Iu-PS接口是由RANAP协议控制的。

传输数据时,GTP-U控制实体必须要与其他协议实体互通。在GGSN中,GTP-U协议实体与位于UMTS网络边缘(例Gi接口)的分组中继功能相联系。在SGSN的Iu-PS侧,GTP-U协议实体同Gn侧的另一个GTP-U实体相联系。在RNC中,GTP-U实体终止隧道,并把分组转交给无线网络层的帧协议实体。

GTP-U同相邻协议实体的互通非常简单,因为控制平面事先已经协商了同用户数据分组传输有关的所有参数。用户数据分组只是被简单地传输到下一个实体,后者再根据预定的PDP报文参数处理分组。

GTP-U协议的主要功能如下。

- 数据分组传输。
- 封装和隧道。
- 数据分组排序。
- 路径生存检验。

用户数据分组最大为1 500 B。包含1 500 B或稍少字节数的用户数据分组可以

作为一个分组来传输。如果从外部网络通过 GGSN 接收到的用户数据分组数超过 1 500 B，GGSN 将根据 PDP 类型分割或丢弃该分组。由于 IP 分割效率低且不能容错，所以应该尽量避免分割。这样包含 GTP-U 的网元间所有链路的 MTU 值在加 GTP-U、UDP 和 IP 头后应该超过 1 500 B。

每个用户数据分组在传输到 UMTS 分组域网络之前要进行封装，把包含隧道信息的 GTP 协议头加入到每个用户数据分组中。隧道信息包含 32 bit 的 TEID（隧道端点标识码）。隧道端点标识码有两个重要作用，一个功能是用于对隧道端点中的 PDP 报文进行寻址，这样也就直接指示了不同的 UE，因为在 UMTS 网络中，一个 UE 可将一个或多个 PDP 报文激活。另一个功能是把具有不同地址的用户数据分组复用为一个由两个 IP 地址标识的单独路径。

GTP-U 可以选择保留 RNC 和 GGSN 之间用户数据分组的顺序。在控制平面的 PDP 报文建立过程中，重排序可以被协商。如果用户数据分组使用了重排序协商，GTP 头就将包含 16 bit 的序列号，用于让 GTP-U 确定用户分组是否已经按正确顺序接收或是否需要因为丢失的分组而等待。不过当未等到的用户数据分组丢失时，这样的数据分组排序机制不能恢复丢失的分组，由其他层负责恢复。

GTP 可以通过定时向对等端 GTP 发送回音请求消息来检查对方是否存活，对方将以回音响应消息来应答。在 Gn 接口，人们可能会认为路径存活的检查过程属于 GTP-C，但因为 GTP-U 是 Iu-PS 接口上唯一的 GTP 实体，故需要由它来处理。Gp 接口的路径存活检查类似于 Gn 接口。

UMTS 网络使用 GTP-U，主要用于 UTRAN 和 SGSN 之间以及 SGSN 和 GGSN 之间的用户分组数据传输。当路由区更新过程需要把 GTP-U 隧道从一个 SGSN 切换到另一个时，GTP-U 用于把还没有发送到 UE 的用户数据分组从旧的 SGSN 中继到新的 SGSN。GTP-U 也是 SRNS 重定位过程的一部分，该过程是指经过一对和 RNC 相关联的 SGSN，把未传输到 UE 的用户数据分组从源 RNC 以隧道方式传送到目标 RNC。

GTP-U 协议定义在 3GPP TS 29.060 中。

10.4 无线网络协议

在 UMTS 互通协议体系（如图 10.4 所示）中，无线网络协议由前述的传输网络协议顶层的下一层协议构成。无线网络层从 UE 扩展到整个 UTRAN，并且在 CN 的边缘节点终止。无线网络协议用于控制无线接入承载的建立、维护和释放，以及用无线接入承载在 UE 和 CN 间传输用户数据。

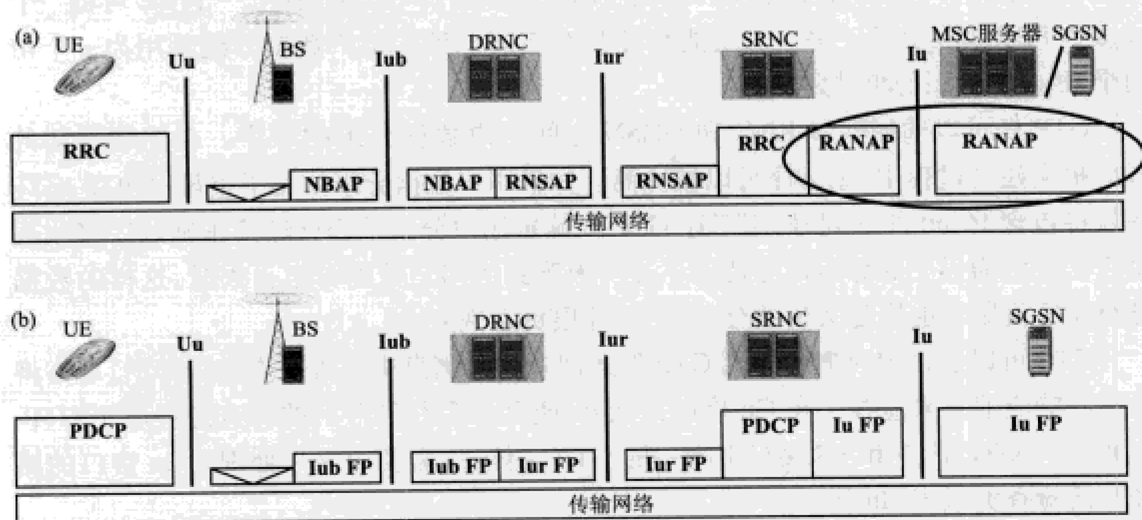
10.4.1 无线网络控制平面

无线网络层中的控制平面协议执行 RAB（无线接入承载）需要的所有控制。根据应用于整个 UTRAN 控制平面设计的客户端—服务器方式，这些协议可以实现无线资

源的管理决定并对所有 UE 进行 RAB 维护，即使它们在 UTRAN 区域中移动时也可以实现。

10.4.1.1 RANAP(无线接入网络应用协议)

Iu 接口连接 UMTS 无线接入网和 CN，同样的 Iu 接口还把电路域和分组域的业务连接到 UTRAN(如图 10.20 所示)。Iu 接口已经设计为可支持 UTRAN 和 CN 技术的独立演进。除此之外，还可以在不改变 Iu 接口的情况下，独立发展核心网的 CS 和 PS 业务，并用相同的 Iu 接口连接到 UTRAN。



(a)传输网中的控制平面协议；(b)传输网中的用户平面协议(只在 PS 域)

图 10.20 无线网络——RANAP

UTRAN 期望到 CS 和 PS 的连接尽可能相似。因此，在 UTRAN 和 CN 间定义了单独的信令协议，称为 RANAP(无线接入网络应用协议)，定义在 3GPP TS 25.413 中。CS 域和 PS 域都使用 RANAP 协议接入 UTRAN 提供的业务。

RANAP 是控制 Iu 接口资源的协议。RANAP 实体存在于 RNC 中，其对等的实体在 MSC 或 SGSN 中。

RANAP 位于 Iu 信令传输层的顶层，在 Iu 接口上使用信令传输业务来传输 RANAP 消息。传输协议栈由几个协议层组成，但最高层总是 SCCP。虽然有两种传输选择(ATM 或 IP)，但总是由 SCCP 实体为 RANAP 提供传输协议栈的业务接口。

RANAP 对底层的传输层有一定的要求。其基本的要求是假定 RANAP 发送到对等端实体的每个消息(PDU)将无差错地到达对等端实体。也就是说，传输协议栈要为 RANAP PDU 提供在 Iu 接口的可靠数据传输。

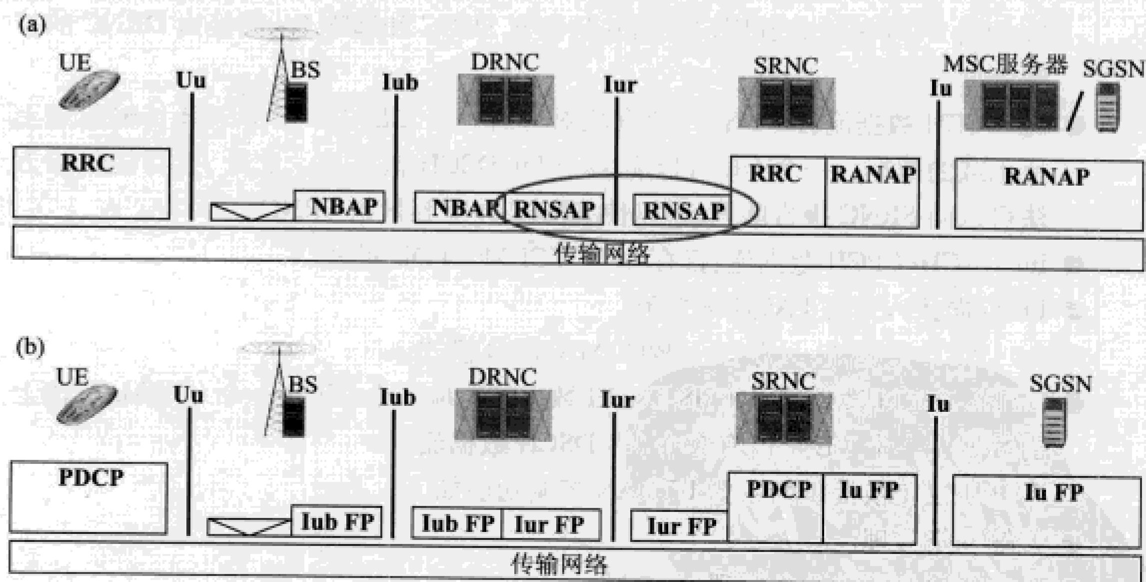
专用控制服务的每个 PDU 应该在单独的信令连接上传输。在 Iu 接口，信令连接由 Iu 信令承载来实现。传输层应能为 RANAP 提供这样一种方式，即在 Iu 接口根据 RANAP 的请求来动态建立和释放信令承载。每个激活的 UE 都有自己的 Iu 信令承

载，由传输层负责维护。如果由于某些原因承载断开，SSCP 将会把有关信息通知给 RANAP。

RANAP 为高层协议提供业务：在 MSC 服务器和 SGSN 侧，非接入层协议使用 RANAP 业务。通过 RNC 中的 RRC 协议互通，RANAP 在 UE 和 CN 之间传输高层协议的信令消息。

RANAP 业务分成两组：通用控制业务和专用控制业务。通用控制业务同 RNC 和 CN 之间的整个 Iu 接口相关。专用控制业务支持 Iu 接口上对 UE 的区分，总是同单独一个 UE 相关。RANAP 主要提供专用业务，所有专用控制业务的 RANAP 消息在专用连接上发送，这种专用连接称为信令连接。

总体 RAB 管理是 RANAP 提供的主要业务之一。RANAP 为 CN 提供在 UE 和 CN 之间建立、改进和释放 RAB 的控制方法。此外，当 UE 从 SRNS 的区域移动到新的区域时，RANAP 通过把 RAB 传输到新的 RNS 来支持 UE 的移动性，这种业务叫 SRNS 重定位。在 UTRAN 中，另一个 RANAP 业务控制着安全模式，所有的这些业务都是专用的控制业务。



(a)传输网中的控制平面协议；(b)传输网中的用户平面协议(只在 PS 域)

图 10.21 无线网络——RNSAP

通用控制服务仅用于一些特殊情况。例如 RANAP 在用户业务增长太快时能够对 Iu 接口负载进行控制，如果 Iu 接口的任何一侧发生严重故障，RANAP 可以提供复位服务，使整个 Iu 接口初始化，并清除所有激活的连接。

RANAP 协议的详细内容已在 3GPP 标准 TS 25.413 中给出。

10.4.1.2 RNSAP(无线网络子系统应用协议)

RNSAP 是无线网络层上的控制平面协议(如图 10.21 所示)。它提供跨 Iur 接口

的控制信令的交换。RNSAP 由两个 RNC 来使用，一个是服务 RNC(SRNC)，另一个是漂移 RNC(DRNC)。SRNC 实现 CN 的 RANAP 的信令连接。

RNSAP 协议总是工作在 SCCP 协议之上。类似于 RANAP 协议，在 SCCP 之下有两个信令传输选项：有 AAL5 适配层的 ATM 传输，或者是以 SCTP 和 MUA 作为适配层的基于 IP 的传输。作为信令传输，SCCP 为 RNSAP 提供两种不同的模式：面向连接的数据传输业务和无连接的数据传输业务。

RNSAP 负责整个 Iur 接口的承载管理信令，用于建立无线链路，并允许 SRNC 控制那些在 DRNS 中使用专用资源的无线链路。

对于每个 DRNC 和使用一个或多个无线链路来传输三层信令的 UE，RNSAP 协议使用一个信令连接来连接它们。Iur 接口传输的信息可以分成以下几类。

- 无线和移动控制信令：对于那些与 UTRAN 存在连接 UE，Iur 接口能够支持它们在 RNS 间无线接口的移动性，包括对切换、无线资源控制以及 RNS 间同步的支持。
- Iub/Iur DCH 数据流：Iur 接口提供上、下行 Iub/Iur DCH 帧的传输，上、下行 Iub/Iur DCH 帧承载着用户数据并且包含 SRNC 和远端 BS 间经由 DRNC 的控制信息。
- Iur DSCH 数据流：Iur DSCH 数据流对应着一个 UE 在一个 DSCH 传输信道上所承载的数据。一个 UE 可以有多个 Iur DSCH 数据流。此外，接口提供的方法可以向 SRNC 报告队列，可以使 DRNC 分配容量给 SRNC。
- Iur RACH/CPCH 数据流：仅存在于 WCDMA FDD 模式。
- Iur 前向接入信道 FACH 数据流。
- Iur USCH 数据流：只存在于 WCDMA TDD 模式。
- Iur HS-DSCH 数据流：Iur HS-DSCH 数据流对应一个 UE 在一个专用 MAC 流上的数据。一个 UE 可以有多个 HS-DSCH 数据流。

RNSAP 协议交换提供的主要 UTRAN 控制功能如下。

- 传输网络管理。
- 公共传输信道的业务管理，如寻呼。
- 专用传输信道的业务管理，包括无线链路建立、增加、删除和测量报告。
- 下行共享传输信道的业务管理，包括无线链路建立、增加、删除和容量分配。
- 公共和专用测量对象的测量报告。
- SRNS 重定位，当服务 RNS 角色由另一个 RNS 代替时，该功能可以协调 RNS 间的活动。

当 RNSAP 用于建立一个或多个无线连路 DRNC 中的必要资源时，它将参与无线链路的建立过程。并且在这一过程中还会建立信令承载的面向连接的业务。

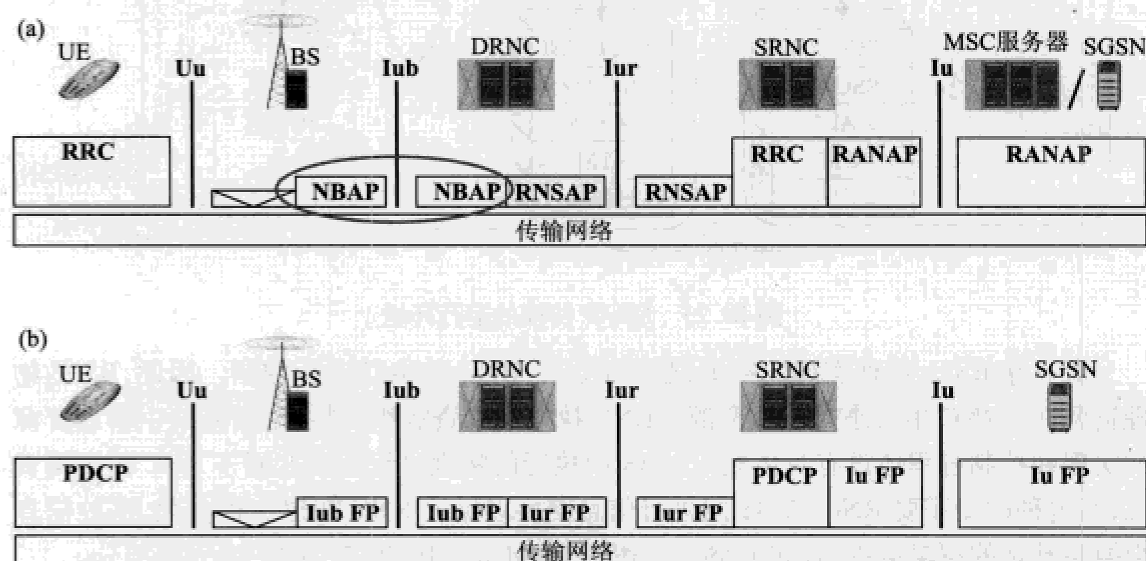
其他 UTRAN 范围内可能需要从 RNSAP 实体获得协议活动的过程有软切换、硬切换、小区更新、UTRAN 注册区域更新与漫游，下行功率控制以及 Iur 接口上 RRC 连接

的释放与重新建立。

对 RNSAP 的全面说明在 GPP 标准 TS25、423 中给出。

10.4.1.3 NBAP(Node B 应用协议)

NBAP 是无线网络层协议,用于维护 Iub 接口控制平面信令,从而控制 Iub 接口的资源并提供 BS 和 RNC 之间的通信(如图 10.22 所示)。NBAP 的一个对等端实体位于 BS 中,另一个位于控制 BS 的 RNC 中(即 CRNC 中)。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.22 无线网络——NBAP

NBAP 位于 Iub 传输层的顶层,使用传输层的服务在 Iub 接口传输 NBAP 消息。3GPP R99 采用 ATM 技术传输 Iub 接口上的 NBAP 信令。ATM 连接同必要的 ATM 适配层一起提供了 NBAP 的信令承载,3GPP TS25.432 中有相应的规定。3GPP R5 标准定义了潜在传输技术中的两个选择:一个是 R99 中的 ATM 连接;另一个是 IP 栈的 SCTP。3GPP R5 标准允许运营商选择两个协议栈中的一个来传输 NBAP 消息。

NBAP 的信令承载提供了可靠的端对端连接。这意味着 NBAP 假定每一个 NBAP 发送给对等端实体的消息都能无差错达到目的地。Iub 接口可能存在多个点到点的 NBAP 信令连接。

BS 自身不对任何无线资源或 RAB 管理进行决策,而是遵循来自 RNC 的命令。NBAP 给 RNC 和 BS 的控制单元提供服务。NBAP 与 RRC 协议同样也有接口,它为 BS 中的 RRC 实体提供可以映射到 BCCH 逻辑信道的信息。NBAP 到 UTRAN 的无线网络层协议没有其他的接口,所有同这些协议的互通都是通过 RNC 的控制单元来实现的。

图 10.23 示出了 NBAP 协议的运行环境,所有 NBAP 的接口在图中以粗体黑色箭头表示。

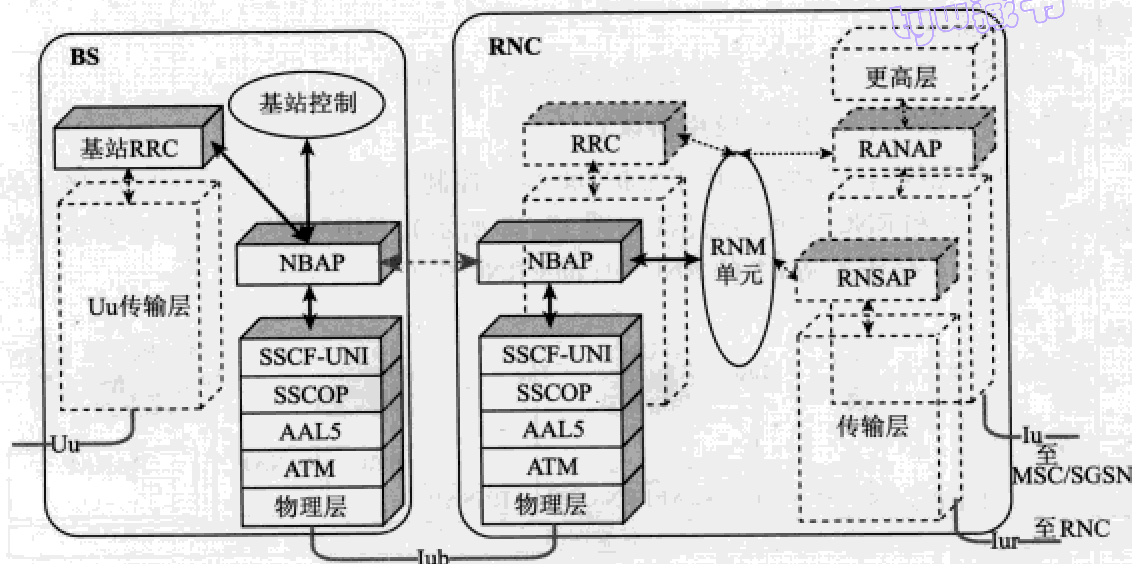


图 10.23 NBAP 协议的运行环境

所有在 BS 上物理实现的资源，逻辑上属于 RNC 并由其进行控制。因此，BS 的物理资源在 CRNC 中看来是逻辑资源。RNC 执行逻辑资源级的控制，而基站中物理资源的实现和控制过程还没有具体规定。BS 中执行的物理过程能改变属于 RNC 的逻辑资源，而这种改变需要 RNC 和 BS 间进行信息交换以保证 RNC 知道这种变化，这种信息交换叫基站的逻辑运维(逻辑 O&M)。逻辑 O&M 是 NBAP 信令的一个完整部分。

NBAP 的另一个重要功能是建立和维护 Iub 接口的控制平面连接，发起建立和释放 Iub 接口专用用户平面连接以及命令 BS 为新的无线链路在 Uu 接口激活资源。所有 NBAP 信令功能都分为公共过程和专用过程。

公共 NBAP 过程是不与任何具体 UE 相关，而是与跨 Iub 接口的公共资源相关。同逻辑 O&M 有关的信令占 NBAP 公共过程的一大部分。NBAP 公共过程包括逻辑资源的配置管理过程以及使 BS 通知 RNC 有关基站中无线资源状况的过程。NBAP 公共过程也允许 RNC 在 BS 内发起特定的测量，然后报告测量结果。除了逻辑 O&M，另一个 NBAP 公共过程用来发送在 RNC 到 BS 的广播信道上传输的信息。NBAP 公共过程也通过建立第一个无线链路为具体的 UE 创建新的 UE 报文并维护 Iub 接口的控制平面信令连接，因此在 Iub 接口总是有一个终止于 BS 公共控制端口的公共 NBAP 信令连接。

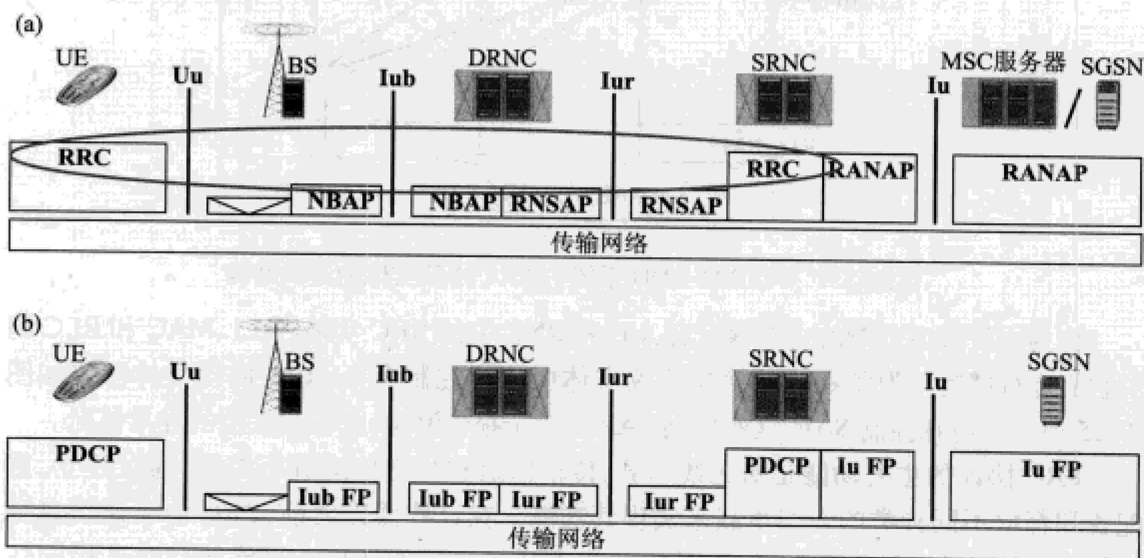
NBAP 专用过程总是同具体的 UE 有关，即总有一个 UE 报文存在于 BS 之中。NBAP 专用过程包括现有无线链路的管理和临视(这些无线链路的 UE 已连接到 BS 上)，这些过程允许 RNC 命令 BS 为某个 UE 报文建立或释放一些无线链路。NBAP 专用过程也使 BS 能够报告无线链路上传输出现了故障或者已经恢复。NBAP 专用过程还提供无线链路重配置管理，支持专用资源和相应功率控制活动的测量，这些测量用于 RNC 调整无线链路上的下行链路功率电平。专用 NBAP 信令由 BS 逻辑模型的一个通信

控制端口来承载,对于跨 Iub 接口的专用 NBAP 过程可以使用几个专用的信令连接。

RNSAP 协议的完整规范在 3GPP TS25.433 中给出。

10.4.1.4 RRC(无线资源控制)协议

RRC 协议是 UTRAN 中关键的无线资源控制协议(如图 10.24 所示)。通过协调资源控制请求,RRC 协议支持在第 5 章所讨论过的 RRM 功能,资源控制请求的协调是基于 RRM 算法的决策。在 RRC 协议的协助下,RRM(无线资源管理)决策的作用可以扩展到所有受该决策影响的 UTRAN 网络单元。RRC 协议消息也在其负荷中承载所有属于非接入层协议的信令。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.24 无线网络——RRC

RRC 协议在 UE 和 RNC 之间使用。RRC 协议实体使用由 RLC 子层提供的信令承载来传输信令消息。RLC 的三种模式在图 10.25 中以不同的 SAP(业务接入点)来表示。例如,当 UE 必须在建立了一个全 RRC 连接(如初始接入或小区/新小区中的 URA 更新)之前和与 RNC 通信时将使用透明模式 TM-SAP。TM-SAP 也用于频繁的重复消息,如寻呼消息,这样可以避免不必要的开销。当需要进行可靠的消息交互时,要使用确认模式 AM-SAP 来控制具体的信令。另一方面,非确认模式 UM-SAP 用于避免确认模式中信令潜在的延时(比如当释放 RRC 连接时,释放消息要通过 UM-SAP 重复多次,此即快速重复功能,可以提高 UE 接收到消息的概率)。

图 10.25 也给出了 RRC 协议实体的逻辑结构。DCFE(专用控制功能实体)用于处理同与 UE 有关的所有信令。对于 SRNC,每个同该 RNC 存在 RRC 连接的 UE 都有一个 DCFE 实体。PNFE(寻呼和通知实体)用于处理那些发送给空闲模式 UE 的寻呼消息。在一个 CRNC 中,所控制的每个小区至少有一个 PNFE 实体。BCFE(广播控制功能实体)处理在 BCCH 和 FACH 逻辑信道上广播的系统消息,CRNC 中的每个小区

至少有一个 BCFE 实体。除了这些功能实体,图 10.25 还包含一个具体的 RFE(路由功能实体),它的功能是在 UE 侧为非接入层消息到不同的 MM/CM 实体进行选路,以及在 RNC 侧为非接入层消息到不同的 CN 域进行选路。

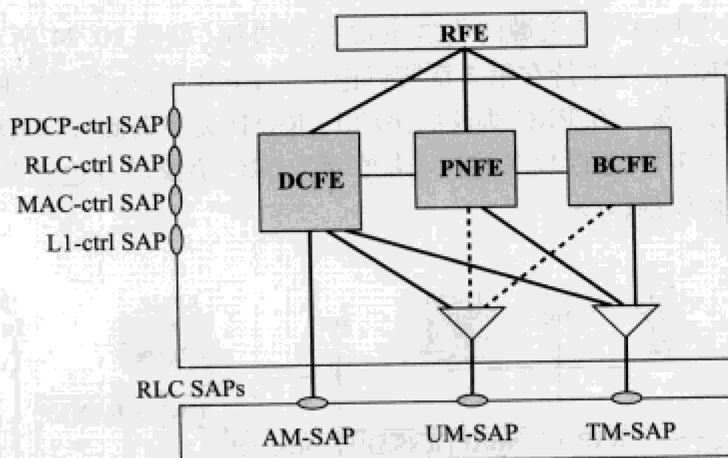


图 10.25　WCDMA-FDD 系统中 RRC 协议实体的逻辑结构

作为无线资源分配的主要执行者,UE 和 RNC 中的 RRC 实体在 L1、MAC 和 RLC 则对它们进行控制。为了在这些底层协议实体中执行控制命令,RRC 协议实体需要如图 10.25 所示的特殊控制 SAP,这些控制 SAP 也用于报告测量,并检测底层的异常情况。

RRC 协议的主要功能是对无线承载、传输信道和物理信道进行控制,通过建立、重配置和释放不同种类的无线承载来实现其功能。在这些操作之前,RRC 协议通信自身首先要使用几个(至少四个)信令无线承载来开始自身的通信。最终的信令连接同任何其他随后建立的承载一起被称为 RRC 连接。在 RRC 连接期间,用户平面业务的其他无线承载的建立、重配置和释放,是通过在信令无线承载上交换对等端 RRC 实体间的命令和状态信息来进行的。RRC 连接会一直存在,只有当所有用户平面承载已被释放,而且 RRC 连接处于 UE 和 RNC 之间时,才会被释放。

无线承载所使用的安全机制是根据 RRC 协议实体的控制激活或非激活的。除了通过加密来激活保密性保护,RRC 协议还能够保证所有高层消息和 RRC 信令消息的完整性。这一点如第 9 章所述,是通过给每个 RRC PDU 增加 32 bit 的消息鉴权码来实现的,该消息鉴权码是由 RRC 实体自身进行计算和校验的。这种方法能保证接收 RRC 实体能够核查出信令数据未被修改过,而且这些数据确实来自于已声明的对等端实体。另外,改变这些功能所用密钥的操作由 RRC 协议根据来自 CN 的指令来执行。

UE 在 UTRAN 级的 MM(移动性管理)是由 RRC 信令控制的。这种由 RRC 协议执行的 MM 功能有:小区更新、URA 更新和激活集更新,这些都在第 5 章讨论过,并会在后续的第 11 章中给出例子。

无线测量的控制及报告由 RRC 协议来提供。在 UE 端,总共可以激活七种不同种类的测量,其中包括 UE 的定位测量。通过各种更进一步的测量,每一种测量可以被单

独控制和报告。

除了上面提到的以外，RRC 协议的功能还包括系统消息广播、UE 的寻呼和交换功率控制参数。

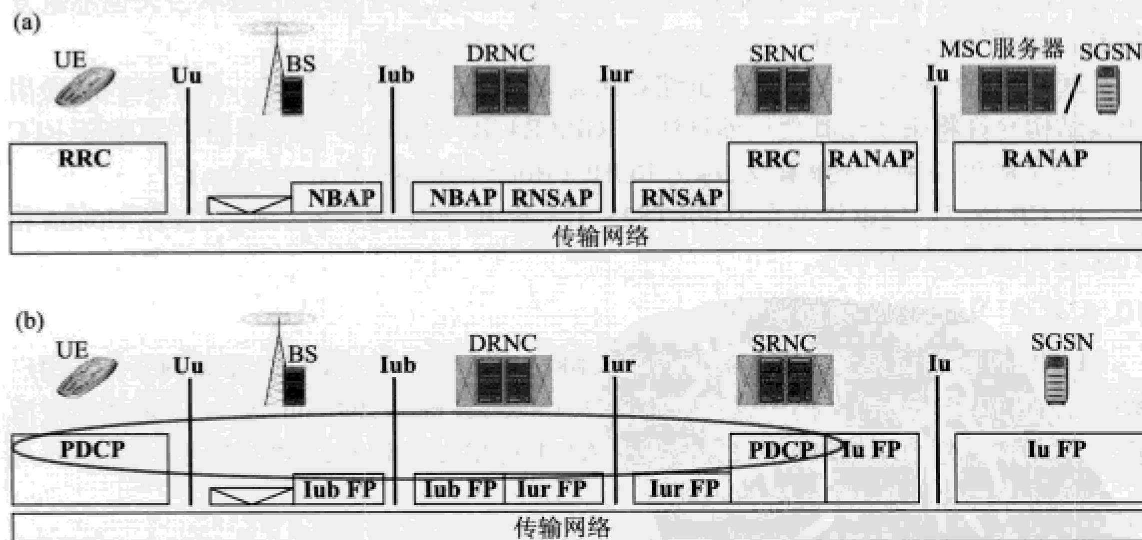
作为一种协议，RRC 协议是相当复杂的，它总共有 40 多种不同的过程和 60 多种不同的 PDU。

RRC 协议的规定在 3GPP 标准 TS25.331 中。

10.4.2 无线网络用户平面

10.4.2.1 PDCP（分组数据会聚协议）

顾名思义，分组数据会聚协议（PDCP）用于使 WCDMA 无线协议适合于传输最常见的用户到用户的分组数据协议——TCP/IP，如图 10.26 所示。因此 WCDMA 无线接口两侧的 RNC 和 UE 都有 PDCP 协议实体。PDCP 协议的核心功能是压缩负载协议头，如果不进行压缩，会浪费宝贵的无线链路容量。例如，对 IPv4 来说，如果不进行头压缩，RTP/UPD/IP 头至少有 40 B；而对 IPv6 来说，至少有 60 B。由于在诸如 IP 语音服务上的净荷大概只有 20 B 或更少，所以如果不压缩的话，开销是很明显的。



（a）传输网中的控制平面协议；（b）传输网中的用户平面协议（只在 PS 域）

图 10.26 无线网络用户平面——PDCP

在 3GPP 无线接口协议模型中，PDCP 属于无线链路层（L2），它的最高子层专用于携带分组数据的用户平面无线承载。

PDCP 协议利用 RLC 层在三种不同模式下的服务。从概念上讲，这些服务可用于三种不同的服务接入点（SAP）上。

- 确认模式数据传输（AM-SAP）。
- 非确认模式数据传输（UM-SAP）。

● 透明模式数据传输(TM-SAP)。

PDCP协议假定分割和重组是由下层的RLC层来执行的,如果要支持无损SRNS重定位,那么PDCP就要使用AM-SAP并且假定RLC SDU能够按顺序传输。

如果要请求可靠数据传输,PDCP就会使用AM-SAP。在这种情况下,RLC层仅允许丢弃某些RLC SDU,但能够在发送方和接收方都能指示每个丢弃的RLC SDU的PDCP。之所以要进行指示,是因为PDCP是压缩协议,它避免在空中发送明确的序列号,而是采用了虚序列号,因此有必要让PDCP知道RLC连接的复位、无线承载重配置,特别是在执行无损SRNS重定位时。

对于TM-SAP,期望的PDCP PDU大小是固定的,这就意味着对高层协议(如IP协议)的PDU大小或IP头压缩都在严格的要求。在一般情况下,分组域的高层或现有的IP头压缩都不能满足上述要求。因此应谨慎使用TM-SAP。

RNC中运行的PDCP协议实体必须同UTRAN帧协议共同完成分组数据中继,其中,下行方向的中继中从Iu到Iub/Iur,上行方向的中继是从Iub/Iur到Iu。一般情况下,中继就是把分组简单地复制到另一个接口,同时执行特定的头压缩和解压缩。如果要执行系统间切换或无损的SRNS重定位,情况则会变得复杂。因此PDCP协议要有特殊的规则用于Iu接口帧协议和RRC协议的互通,从而保证分组不丢失也不重复传输,分组序列号在切换或重定位后在目标系统中能够恢复。

3GPP R99规定的唯一IP头压缩算法是IETF定义的RFC2507。但PDCP的通用协议结构允许将来使用其他压缩算法。3GPP R4/R5对PDCP规范增加了由IETF RFC 3095定义的另一种头压缩算法,称为ROHC(Robust Header Compression)。

PDCP协议的完整规范在3GPP TS25.323给出,如需进一步了解,可参阅Holma和Toskala的著作(2004年)。

10.4.2.2 UTRAN帧协议

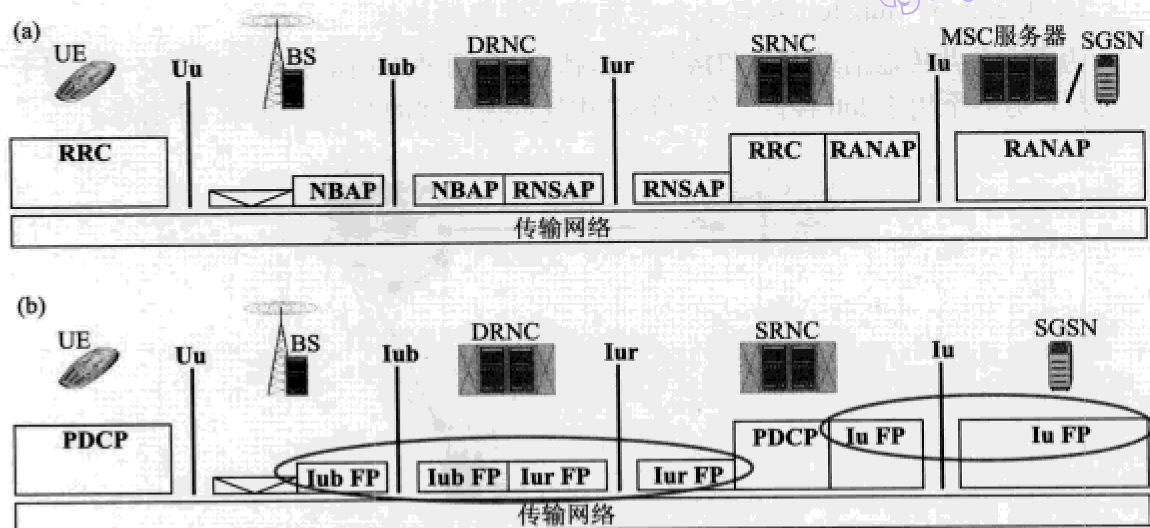
UTRAN帧协议是无线网络层用户平面协议,用于在公共UTRAN承载网络传输用户数据(如图10.27所示)。帧协议在所有UTRAN接口(即Iu、Iub、Iur接口)上都处于激活状态。帧协议使用的传输网络服务是基于ATM或IP协议栈的,这些内容见10.3.3节。

10.4.2.2.1 Iu接口的帧协议

在Iu接口处的帧处理协议既可用于电路域的用户数据传输,也可用于分组域的用户数据传输。由于两个域的传输业务不同,所以要使用两种Iu帧协议模式。

● 透明模式用在不需要任何特殊协议活动(如组帧)的RAB上。因此透明模式下数据只是简单的通过传输网络而不需要增加任何协议头信息。透明模式因此就是一个空协议。透明模式可用于从RNC到SGSN或在相反方向上以GTP-U格式传输非实时的数据分组。

● 支持模式是一个具有控制PDU和用户数据组帧的完整协议。这些协议用于CS域中承载AMR语音的RAB。因此支持模式的控制PDU能够执行实时语音传输所需要的速率控制和时间同步。在这种情况下,支持模式协议直接使用传输网络提供的AAL2服务或RTP会话。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在PS域)

图10.27 无线网络用户平面——UTRAN帧协议

10.4.2.2.2 Iur/Iub接口上专用信道的帧协议

图10.28中示出了Iur和Iub接口上专用信道的公共帧协议。SRNC能够通过该协议同那些由SRNC自身或远程BS提供服务的UE进行用户数据帧交换。除了一般的上、下行数据传输,帧协议还有许多控制功能,这些功能可以执行时间调整和同步,外环功率控制命令和其他UE需要知道的无线接口参数更新也在专用信道帧协议消息中发送。

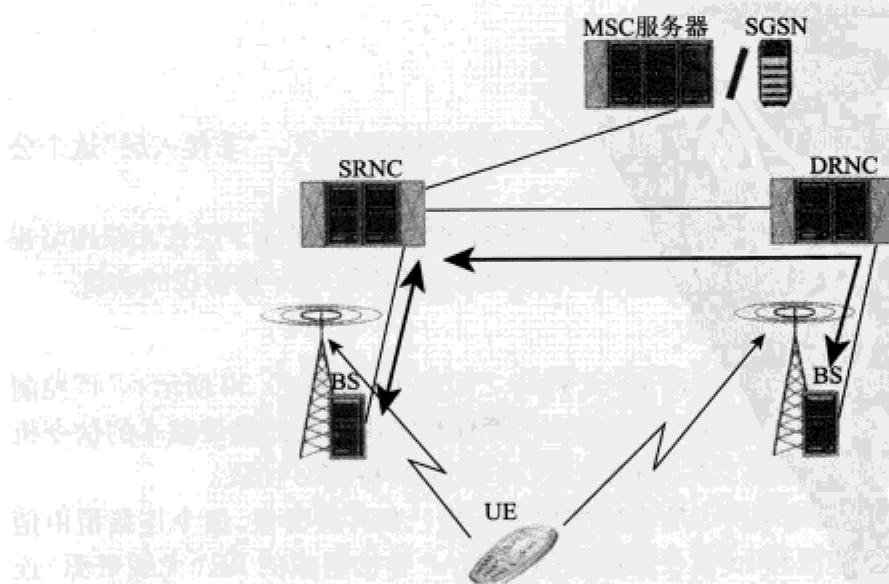


图10.28 Iur和Iub接口上专用信道的帧协议

10.4.2.2.3 Iur/Iub 接口上公共传输信道的帧协议

为了在公共传输信道发送和接收数据帧，需要两种不同的帧处理协议：一个用于 Iur 接口，另一个用于 Iub 接口。在 DRNC 中这些协议间的互通如图 10.29 所示。

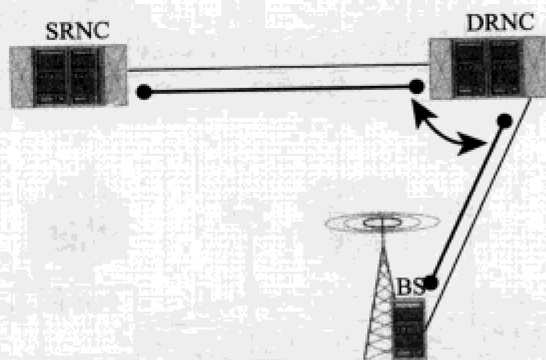


图 10.29 Iur/Iub 接口上公共传输信道的帧协议

除了同具体传输信道类型有关的上下行链路数据传输，这些帧协议还执行一些控制任务。Iur 接口使用基于信用的帧协议处理流控制。在 Iub 接口的帧处理功能包括同步和时间调整及其对 HS-DSCH 的流控制。

10.5 系统网络协议

当无线网络协议能够通过 UTRAN 子网进行通信，并能维护到移动终端的通信路径之后，就由系统网络协议建立到终端用户的通信业务。系统（网络）协议运行于无线网络协议的上层，在 UNTS CN 之中。

10.5.1 非接入层协议

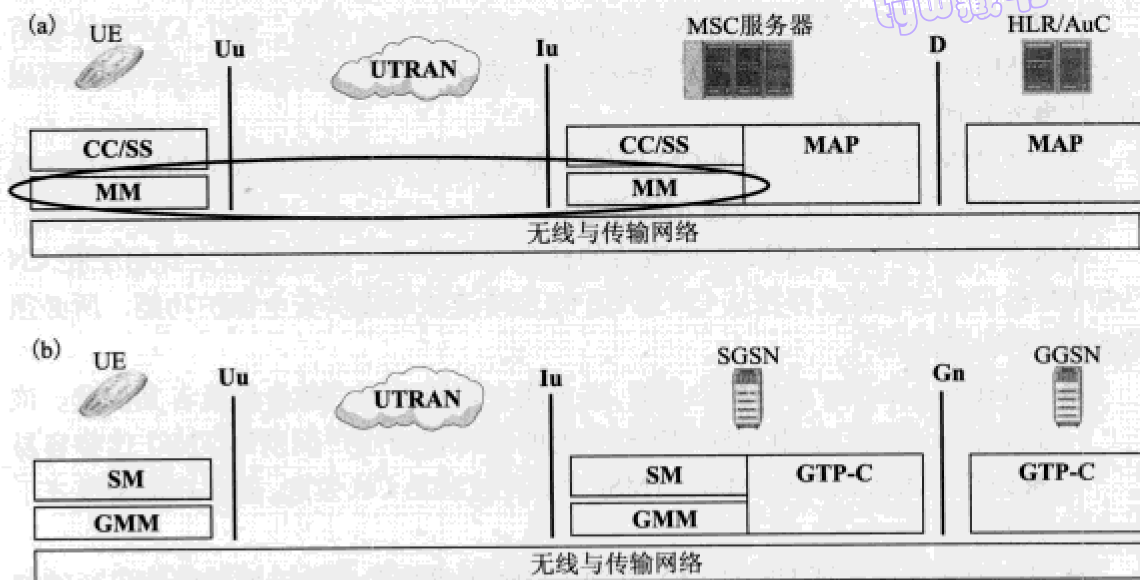
非接入层指用于控制 UE 和 CN 间通信的一组控制平面协议。“非接入层”这个公共名称说明它们是以透明方式通过 RAN 的。

这一组中的协议属于图 10.3 所示的系统网络的两个子层。MM 子层在无线网络提供的信令连接之上。除了自身的功能，MM 子层也可以作为到 CM 子层协议的承载。

10.5.1.1 电路交换域 MM 协议

MM（移动性管理）协议在 UE 和 MSG/VLR 之间使用（如图 10.30 所示）。该控制平面协议为控制 UE 和 CN 电路域之间的移动性管理和鉴权功能提供最基本的信令机制。支持 PS/CS 两种模式或仅支持 CS 模式的 UE 都能支持 MM 协议。

MM 协议利用无线网络层协议所提供的信令连接。在有些时候，信令连接指由信令无线承载上的 RRC 连接和 Iu 信令承载上的 RANAP 连接组成的 RR（无线资源）连接。在任何 MM 协议活动激活前，首先要建立信令连接。在 CN 内，MSC/VLR 侧的 MM 协议实体必须要和 MAP 协议互通才能维护在 HLR 中的位置登记。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在PS域)

图10.30 系统网络非接入层——CS模式的MM协议

MM协议控制着UE以及网络侧相应对等端实体的MM状态。这些协议实体的主要状态用来指示那些对UE使用CM子层业务能力有重要影响的UE位置更新状态。这也就是MM协议用来在UE和MSC/VLR之间传输CM子层协议消息的原因。

MM协议有三个主要的过程。

- MM连接过程。
- MM公共过程。
- MM特殊过程。

MM连接过程除了用于建立和释放MM连接之外也用于传输CM子层消息。MM连接的概念不需要交换任何特殊的MM协议初始消息就能建立,相反,MM连接的建立和释放则要根据来自CM实体的请求。

当UE发起了MM连接的初始化后,MM协议实体发起包含下列参数的CM SERVICE REQUEST。

- UE标识码(如TMSI)。
- 移动台类型码2。
- 密钥序号。
- CM服务类型,用于识别请求的事务类型,如移动台发起的呼叫建立、紧急呼叫建立、短消息或补充服务的激活等。

在CN侧的MM协议实体收到这种请求后将分析这些参数并且决定对服务请求的批准和延续。

另一方面,建立MM连接的请求可以来自网络侧的CM实体,然后通过寻呼过程使UE建立MM连接来处理请求。

MM 连接建立后，CM 子层实体可以使用它来进行信息传输。每个 CM 实体都有自己的 MM 连接。这些不同的 MM 连接由 PD(协议识别符)来区分，更进一步还可以由 TI(事务处理标识)来区分。

建立的 MM 连接可以由本地 CM 实体来释放，然后对连接的释放由 MM 子层来执行，也就是说在无线接口无需传输 MM 消息。

MM 公共过程可以在 MM 连接激活的任何时候发起。这些过程主要用于在 CN 已知 UE 标识和位置以及存在从 CN 到 UE 的 MM 连接时提供安全保护功能。所必须的 MM 公共过程如下。

- TMSI 再分配用于保护用户身份，防止他人识别出用户的身份或者其位置。该过程在无线接口上用 MSC/VLR 分配的临时移动用户识别码 TMSI 代替容易被跟踪的永久识别码 IMSI。TMSI 再分配过程由 CN 发起，通常在加密模式下运行。
- 鉴权使 CN 能验证 UE 的身份，并向 USIM 提供相关参数以使其能算出新的加密密钥和完整性密钥。UMTS 网络对鉴权过程进行了扩展，可以允许 UE 对 CN 进行鉴权(见第9章)，这样做例如可以使 UE 能发现伪基站。鉴权过程总是由 CN 发起的。
- 识别过程用于 CN 要求 UE 为网络提供具体的标识参数，如 IMSI 和 IMEI。
- IMSI 离线过程由 UE 发起，发生在 UE 不再激活或者 USIM 从 UE 分离时。每个 UMTS 网络可以在系统信息块中广播一个标识，用来指示 UE 是否需要此过程。收到 MM IMSI DETACH INDICATION 消息后，网络为该 IMSI 设置一个未活动指示，不需要对 UE 发响应消息。此后，网络将释放本地任何正在进行的 MM 连接，并开始正常的信令连接释放过程。
- 中断过程用于 CN 中止正在建立的或者已经存在的 MM 连接，发生在网络故障或发现非法 ME 时。

MM 特定过程用于处理位置更新消息。第11章给出了位置更新过程中的一个消息流示例。有三种基本的位置更新过程。

- 正常位置更新用在 UE 发现其位置区发生变化时，此时需要向 CN 通知自己新的位置。位置的变化是通过比较系统广播的位置区识别码(LAI)和 USIM 所存储的当前 LAI 来判断的。如果某个服务请求从 VLR 得到的响应 UE 未知，也会启动正常位置更新。UE 必须根据位置更新的失败情况在 USIM 中维护一个“禁止漫游位置区”列表。
- 定期位置更新根据 UE 中的定时器定期向 CN 通知其可用性和位置。定时器的超时值来自广播的系统消息块。
- IMSI 连线过程发生在 UE 进入或切换到一个网络但位置区又是刚刚离线的位置区的时候，即当前小区广播消息中的 LAI 同当前在 USIM 中的 LAI 相同时。

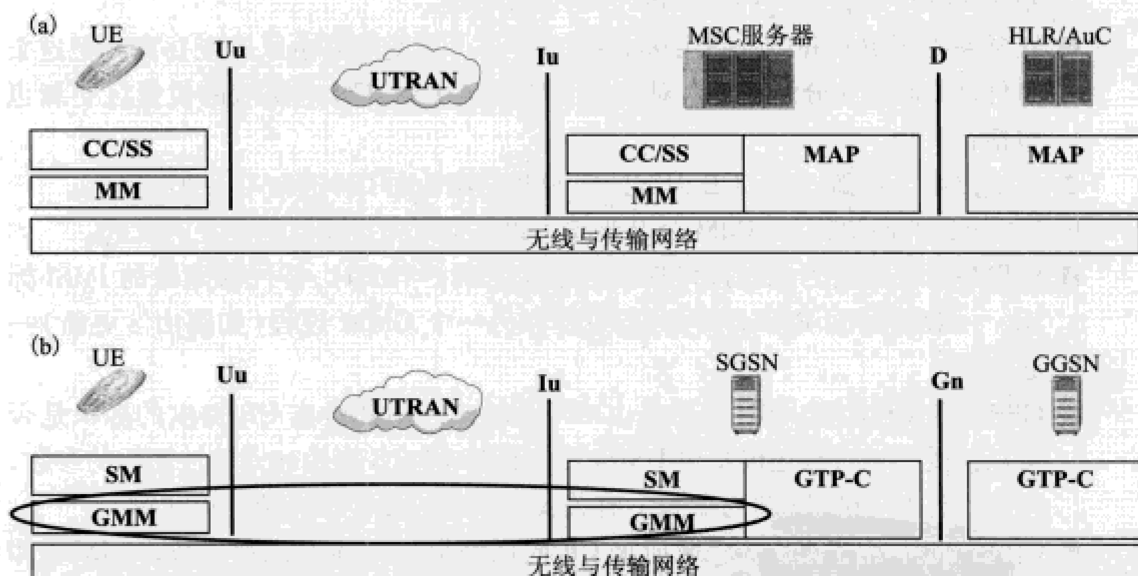
MM 特定过程的公共特性是，仅当没有其他 MM 特定过程正在运行或者没有其他

MM 连接存在时，才能发起 MM 特定过程。还应注意，上述 MM 公共过程中除 IMSI 离线外，都可以在 MM 特定过程期间发起。

由于 MM 协议是从 GSM 相应的协议直接扩展而来的，所以想对此有更多了解的读者可以参考任何书后列出的有关 GSM 的参考文献。MM 协议的完整规范和 UMTS 细节见在 3GPP TS 24.008。

10.5.1.2 GPRS 分组域移动性管理(GMM)

GMM 工作在 UE 和 SGSN 之间(见图 10.31)。其名称是因为它基本是从 GSM/GPRS 系统相应的 PS 业务协议演进而来的。这个控制平面协议为 UE 和 CN 分组域间的 MM 控制和鉴权功能提供最基本的信令机制。能支持 PS/CS 两种模式或仅支持 PS 模式的 UE 都能支持 GMM 协议。



(a)传输网中的控制平面协议；(b)传输网中的用户平面协议(只在 PS 域)

图 10.31 系统网络非接入流——PS 模式的 MM 协议

类似 MM 协议，GMM 协议利用了 UE 和 SGSN 之间的信令连接。这个信令连接常常称为 PS 信令连接，它是由在信令无线承载上使用 RRC 的传输网络层协议和 Iu 信令承载上的 RANAP 来提供的。在 SGSN 侧的 GMM 协议实体必须同 GTP-C 协议实体互通来交换位置信息。

在 PS/CS 模式下工作的 UE 可能同时存在和 MSC/VLR 以及 SGSN 的信令连接。出于优化的考虑，在这种情况下 UE 的 GMM 以及 SGSN 中的 GMM 实体要执行一个组合过程。组合 GMM 过程的思想是为了避免当 CN 分组域能够向 CN 电路域通知有关核心网中的组合活动时，既要发送 MM 消息又要发送 GMM 消息。在 CN 侧，可选的 Gs 接口用于实现这一组合。

从分组数据业务来看，很重要的一点是 CN PS 域是否知道 UE 标识及其位置信

息。这是因为分组数据要用用户特定的密钥加密。GMM报文的概念突出了这两种状态的区分在。当CN分组域知道用户的有关信息时，存在GMM报文，否则不存在。

GMM报文建立和释放的GMM的具体过程如下。

- GPRS连线和组合GPRS连线。该过程用于给网络指示用户标识（典型是P-TMSI）和当前网络的路由区并为该用户建立GMM报文。执行该过程的典型情况是UE分组模式开启或USIM的插入。对于组合的GPRS连线过程，则执行一般的IMSI连线过程。
- GPRS离线和组合的GPRS离线。当UE关机或移除USIM，或者当网络发生异常时启用该过程。GPRS离线使UE标记为在CN分组域不再活动，而组合GPRS离线还将在CN电路域标记UE为不活动。

下面的GMM步骤用于存在GMM时的位置管理。

- 正常路由区更新和组合路由区更新：发生在UE发现路由区改变并需要把这个事件通知给CN分组域时。对于组合路由区更新，CN电路域的位置区更新也包括在其内。
- 定期路由区更新：根据UE内部的定时器定期性向CN通知UE的可用性。

出于安全目的而执行的GMM公共步骤可以在GMM报文已经建立时发起。

- P-TMSI再分配：为无线接口提供分组TMSI（P-TMSI），替代易跟踪的IMSI标识。一般情况下，P-TMSI再分配过程和另一个GMM过程（如路由区更新）一起执行。
- GPRS鉴权和加密：该过程总是由CN发起，CN用其检查UE提供的标识是否可以接受。该过程还能提供USIM用来计算UMTS密钥和完整性密钥的参数，并且允许UE对CN进行鉴权。有关安全功能的更详细介绍见第9章。
- GPRS识别：用于CN分组域请求UE向网络提供具体的识别参数，如IMSI和IMEI。在GMM协议的顶层还需要另一个GMM过程为CM子层提供服务。
- 服务请求：该过程由UE发起，用于建立到网络的可靠连接，并请求建立用于数据传输的承载。该过程典型的应用情况是，UE要发送信令消息（如SM或寻呼响应消息），或者要发送需要安全保护的数据分组。

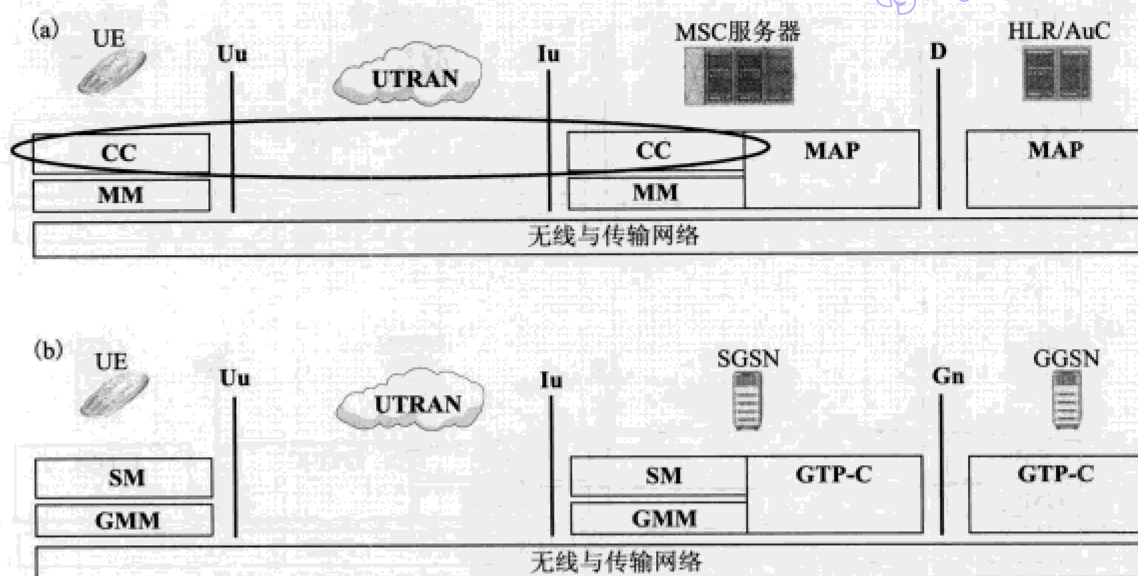
如果要了解更多关于GMM协议的细节，请查阅3GPP标准TS 24.008。

10.5.1.3 呼叫控制（CC）协议

CC协议为建立和释放电路交换业务（如语音呼叫或多媒体业务）提供基本的信令机制（见图10.32）。CC协议工作在MSC/VLR和UE之间，该UE工作在PS/CS模式或仅工作在CS模式。CC协议使用MM子层提供的连接服务传输CC协议消息。

对一般CS语音的控制类似于ISDN电话。因此，GMSC中的CC协议实体必须要和ISUP（ISDN用户部分）协议互通，从而通过外部ISDN网络建立呼叫路径。

UMTS电路交换多媒体呼叫是基于3G-324M的，3G-324M是对ITU-T建议H.324的修改。详细情况请参考3GPP TS26.111。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.32 系统网络非接入层——CC 协议

呼叫建立过程建立了 UE 和 CN 间的 CC 连接,并在必要时激活语音/多媒体编解码和互通功能。MSC/VLR 中的 CC 协议实体要同 RANAP 协议实体进行互通来为电路交换呼叫建立 RAB。这意味着由 CC SETUP 消息中的 CC 协议实体所接收到的 QoS 要求必须要映射到相同 MSC/VLR 中的 RANAP 协议实体的一个 RAB 请求上。只有当 UTRAN 已经确认分配了一个 RAB,呼叫建立才能继续。

建立的呼叫既可以是移动台发起的也可以是移动台终止的。对于多媒体电路交换呼叫来说,一般在其呼叫建立过程中,要在 CC 协议消息中使用一些额外的信息元。而由 UE 或 CN 发起的呼叫释放过程则用来释放呼叫所占用的资源。

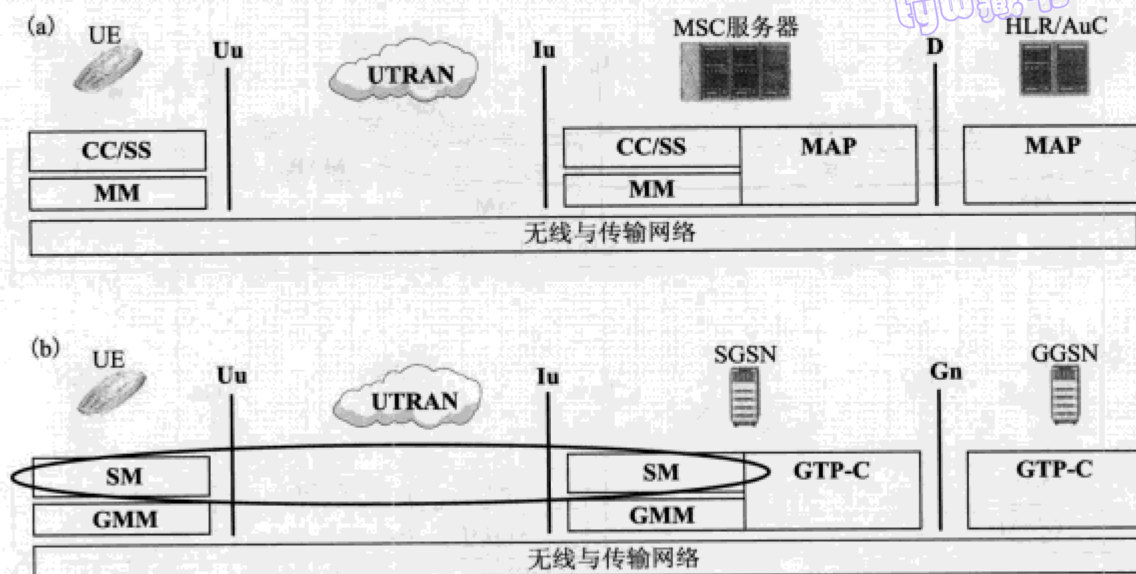
因为任何同时进行的 MO(移动台发起呼叫)和 MT(移动台终止呼叫)在 CC 协议中是分开处理的并且分配了不同的事务标识,所以网络侧不会发生这样的呼叫冲突。

CC 作为网络的核心功能已经在第 6 章讨论过了。第 11 章将给出一个用于电路交换的呼叫建立和释放的消息流的例子。

由于 CC 协议是从 GSM 相应的协议直接扩展而来的,想进一步了解的读者可以参考书后列出的任何有关 GSM 的参考文献。CC 协议的完整规范和 UMTS 细节已在 3GPP TS 24.008 中给出。

10.5.1.4 会话管理(SM)协议

运行 SM 协议的协议实体位于 UE 和 SGSN 中(见图 10.33)。这个协议相应于电路域 CC 协议,用于建立和释放分组数据会话。为了强调 UMTS 网络有可能使用多个分组协议,把这些会话叫作 PDP 报文(见第 6 章)。实际当中需要支持的最重要的分组数据协议是 IP 协议,特别是 IPv6。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.33　系统网络非接入流——SM 协议

SM 协议的主要目的是支持 UE 的 PDP 报文处理。在 SGSN,SM 协议实体与 GTP-C 协议实体在 Gn 接口侧互通,目的是为了把 PDP 报文的管理扩展到 GGSN 中。PDP 报文包括了从 GGSN 到 UE 或相反方向的用于用户平面数据分组路由的必要信息。一个 UE 可以有几个同时激活的 PDP 报文,其中每一个由其自身的 SM 协议实体进行控制。

SM 过程要求所识别的用户存在 GMM 报文。如果没有,MM 子层必须发起 GMM 过程来建立所需的 GMM 报文(见 10.5.1.2 节所述的 GMM 协议)。GMM 报文建立后,SM 协议使用由 MM 子层提供的服务。在 GMM 执行过程中,正在进行的 SM 过程要被暂停。

SM 过程可以由 GGSN 或 UE 发起。基本的 SM 过程如下。

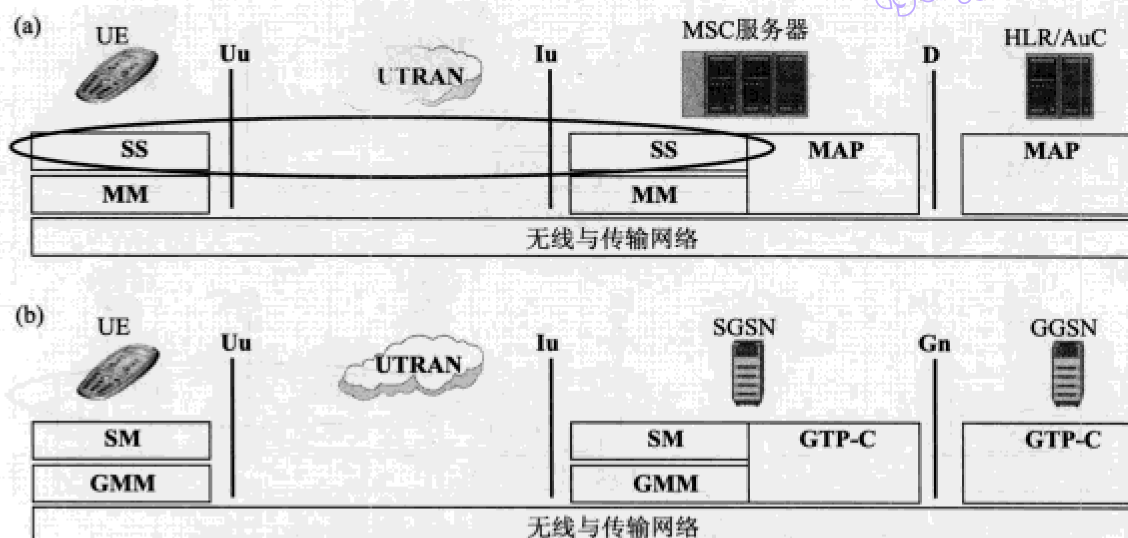
- PDP 报文的激活:在 UE、SSGN 和 GGSN 端建立一个新的 PDP 报文,其中包含会话所需的必要的路由和 QoS 参数。
- PDP 报文修改:发生在会话参数(如会话所需的 QoS 或业务流模板等)改变时。也可以由 UE 或 GGSN 发起。
- PDP 报文去激活:不再需要相应的会话时,用来销毁 UE 和 CN 中的 PDP 报文。

SM 协议的更详细描述在 3GPP TS 24.008 中已给出。

10.5.1.5　补充业务(SS)协议

补充业务是 CS 上提供的附加业务,如图 10.34 所示。补充业务源于 2G GSM 系统,因此工作在 CS 模式的 UMTS 终端可以与 GSM 电话有同样的补充业务。

3GPP 支持 CS 中的各种补充业务。典型的补充业务如下。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在PS域)

图10.34 系统网络非接入层——SS协议

- 不同触发条件的呼叫转移业务,包括无响应时转移、占线时转移、无条件转移、无法接通时转移。
- 各种呼叫禁止业务,包括呼入、呼出、国际呼出和漫游呼叫等。
- 呼叫进行中的业务,如呼叫等待和呼叫保持。

TS 24.080给出了3GPP R99所支持的全部补充业务。

补充业务由SS协议来控制,SS协议是CM子层的一部分。UE和MSC/VLR侧的SS协议实体通过MM连接来通信。这种通信必须处理补充服务的激活和去激活。在CN侧,一旦补充业务命令有要求,比如要访问HLR中的用户信息,SS协议就要同MAP协议进行互通。

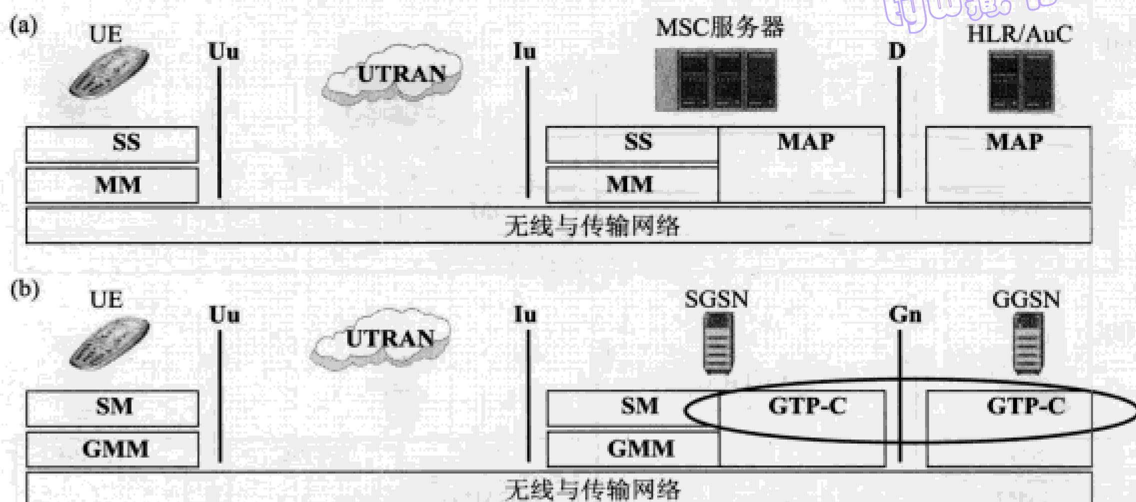
10.5.2 CN节点间的控制平面

10.5.1节简单介绍了UE和CN间非接入层中的控制平面协议。CN实体之间也要执行一些信令功能,特别是CN归属网络中的寄存器。

MAP和CAP协议已经在10.1.3节有所讲述,对细节有兴趣的读者可以参考书后有关GSM的参考文献。3G版本的MAP协议定义在3GPP TS 29.002中。

GTP-C(控制平面GPRS隧道协议)

GTP-C属于CN分组域,位于SGSN和GGSN中(如图10.35所示)。GTP-C是专用于隧道管理和控制过程的控制平面协议。它使SGSN和GGSN能够进行用户数据分组传输。GTP-C也用于在SGSN之间传输GMM信令消息,相当于电路交换侧的MAP/G接口。



(a)传输网中的控制平面协议;(b)传输网中的用户平面协议(只在 PS 域)

图 10.35　控制平面——GPRS 隧道协议

GTP-C 工作在两种不同的接口 Gn 和 Gp 中。Gn 接口是属于 UMTS 分组域的 GSN(即 SGSN 和 GGSN)之间的接口,Gp 接口是两个 UMTS 分组域之间互通的接口(如图 6.4 所示)。

不管是在 Gn 和还是在 Gp 接口,GTP-C 都在 UDP/IP 协议族的顶层运行。UDP 提供(不需要建立连接)无连接消息传输。IP 的主要服务是在源网元和目的网元间进行选路。

在 SGSN 中,GTP-C 协议实体不仅与 Gn 侧的 GTP-U 实体进行互通,而且还要与 GMM 和 SM 协议实体进行互通。在 GGSN 中,与 GTP-C 协议实体互通的有位于 Gn 接口的 GTP-U 实体和 Gi 接口中的外部网络互通功能,如给 PDP 报文分配动态地址。

GTP-C 协议必须在 Gn 和 Gp 接口上可靠地传输信令消息。因此,GTP-C 协议的设计要能够解决由于使用 UDP/IP 传输层而带来的不可靠消息传输的问题。这样,GTP-C 协议中就要包括用于控制和检测消息丢失和重传的定时器以及消息序列号。

10.5.2.1.1　SGSN 和 GGSN 之间的 GTP-C 过程

GTP-C 用于创建、删除和修改 GTP 隧道,GTP 隧道用于传输用户数据分组。另外,GTP-C 协议还用于检测对等端 GTP-C 的路径是否激活。

当 PDP 报文被激活后,SGSN 中的 GTP-C 将发起到 GGSN 的 GTP 隧道建立过程,该过程用于协商 SGSN 和 GGSN 之间与用户数据传输有关参数,参数包含 QoS 以及那些与激活地址有关的参数,如业务流模板。

当 PDP 报文去激活后,GTP-C 协议将从 SGSN 和 GGSN 移走 GTP 隧道信息。

PDP 报文的修改过程能以动态灵活的方式对变化的情况做出反应。当一个 PDP 报文进行修改时(比如由于 QoS 参数改变或负载状况改变而引起的修改),GTP-C 将发起 GTP 隧道修改过程。在此过程中,SGSN 和 GGSN 都能够修改在 GTP 隧道建立协商过程中的大多数参数。PDP 报文的修改过程也作为 SGSN 间路由区更新过程以及

SRNS 重定位过程的一部分，它涉及两个 SGSN，以通知 GGSN 一个新的 SGSN 开始为 UE 提供服务。

网络方面支持对请求 PDP 报文的激活，但 GGSN 并没有必要的协议通过 Gc 接口同 HLR 进行通信，而是用 GTP-C 将消息发送给另一个 GSN，由它在 GTP 和 MAP 之间进行消息转换。然后用 MAP 协议通过 Gc 接口与 HLR 进行通信。GGSN 同 HLR 进行通信的目的是为了发现 UE 是否连接到网络以及得到为 UE 提供业务的 SGSN 的地址。在 GGSN 请求 SGSN 发起 PDP 报文激活过程前，上述信息是 GGSN 所需的。

10.5.2.1.2 SGSN 间的 GTP-C 过程

GTP-C 用于两个 SGSN 之间的通信，目的是交换与 UE 有关的信息。这样的通信发生在 UE 进行 GPRS 连线过程中，或进行 SGSN 间路由区更新过程中，或当 UTRAN 执行涉及两个 SGSN 的 SRNS 重定位过程决策中。

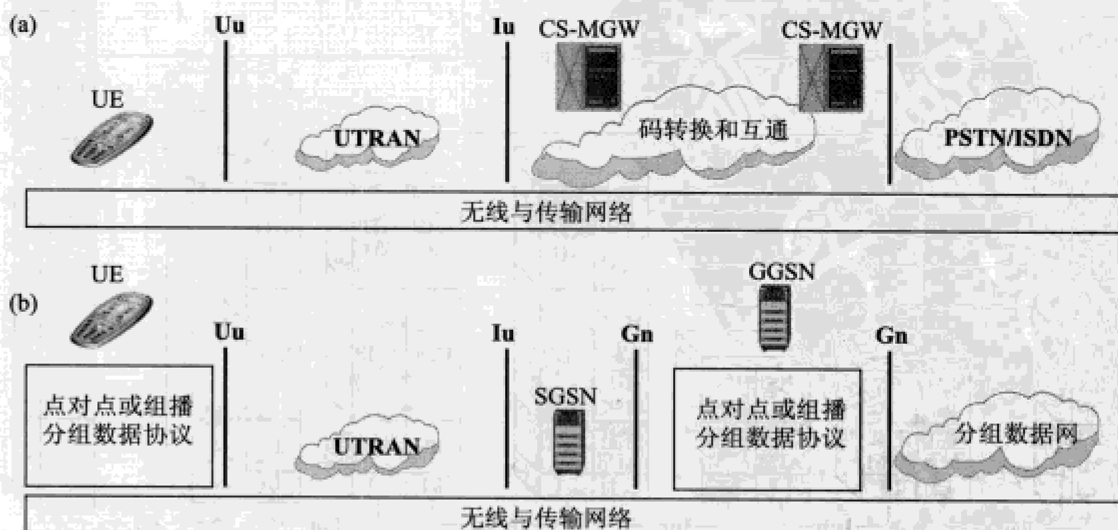
在 SGSN 之间用 GTP-C 交换与 UE 有关的信息可以最小化对无线接口的使用。比如，当执行 SGSN 间路由区更新过程或涉及两个 SGSN 的 SRNS 重定位时，为 UE 服务的新 SGSN 可以从旧 SGSN 接收所有需要的信息。这些信息包括 GMM 相关的参数（如 IMSI 和 GMM 报文）和 SM 相关的参数（如激活的 PDP 报文）。

在 SGSN 间交换 UE 相关信息时，使用 GTP-C 也增加了系统的安全性。比如，当 UE 执行 GPRS 连线过程时，IMSI 可以从旧 SGSN 取回，不用经过空中接口从 UE 获得。

GTP-C 协议定义在 3GPP 标准 TS 29.060 中。

10.5.3 系统网络的用户平面

在 CS 域，用户平面协议的作用由 UE 和服务 MSC/VLR 中的语音编解码承担（如图 10.36 所示）。预定义的语音编码是自适应多速率编码 AMR。除了码转换外，还必须考虑 UMTS 和外部 PSTN/ISDN 之间的互通功能（见第 6 章）。



(a) 传输网络中的控制平面协议；(b) 传输网络中的用户平面协议（只在 PS 域）

图 10.36 系统网络中的用户平面

在 PS 域，UE 和 GGSN 根据一些点对点或组播分组数据协议交换数据分组。最常见的用户平面协议很可能仍旧是 IP 协议。

10.6 UMTS 网络协议总述

前面介绍了所有的主要 UMTS 网络协议，下面对 PS 域协议栈的所有组成进行一下总结，如图 10.37 和图 10.38 所示。

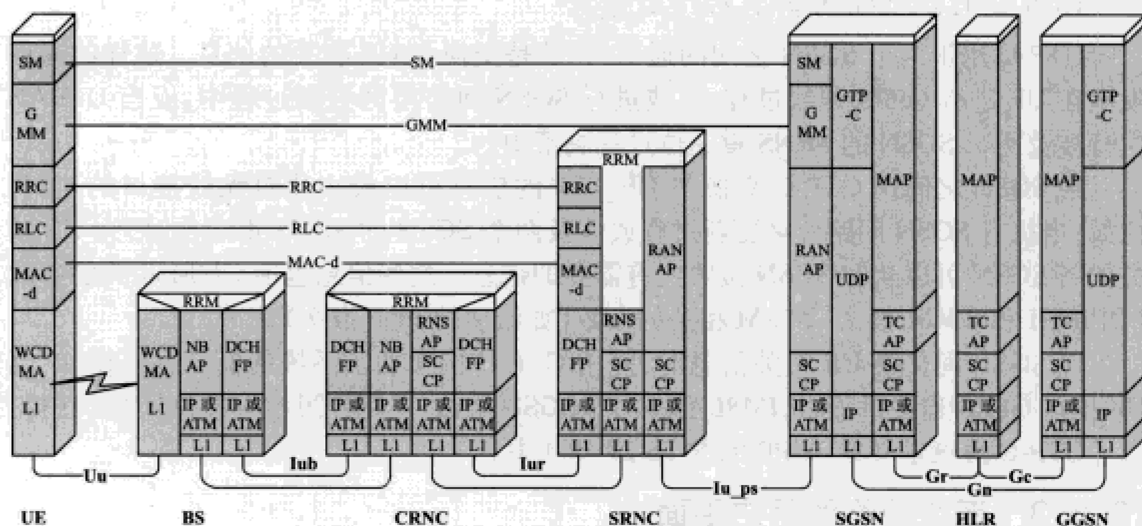


图 10.37 PS 域中控制平面协议栈

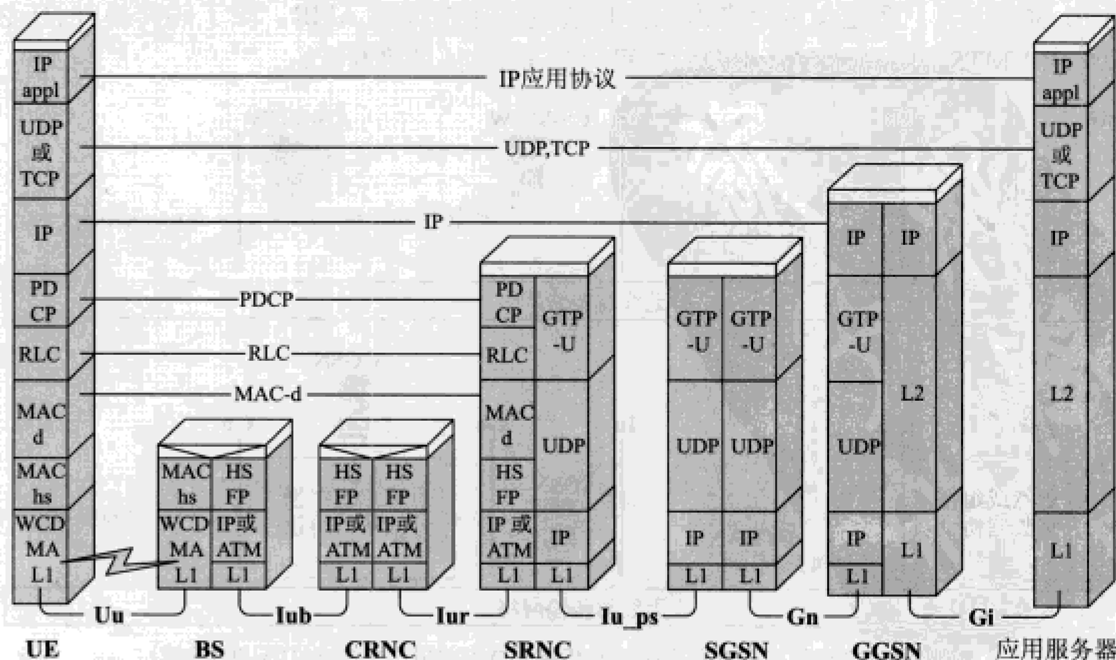


图 10.38 PS 域中的用户平面协议栈

图 10.37 示出了所有 PS 域网元的控制平面协议栈。它给出了典型系统网络级信令过程中活动的控制平面协议(如 PDP 报文激活)。信令承载由 UTRAN 控制协议(RANAP、RNSAP 及 NBAP)和 RRC 协议建立和维护,它们通过相互协作实现分布式无线资源管理。系统网络级控制信令(如 SM 协议消息)通过 RRC 信令消息在 UTRAN 的各单元之间中继。RRC 信令消息又进一步嵌入到 RLC/MAC 和 DCH-FP(专用信道帧协议)消息中。图 10.37 通过 CRNC 处的两个 DCH-FP 协议栈示出了 PLC/MAC 消息的中继。如前所述,所有 UTRAN 接口上的传输可以是 IP 或 ATMIP 传输网络。

CN 侧的 SM 协议和 GTP-C 协议一起控制 PDP 报文。GMM 协议也以类似的方式和 MAP 协议一起实现 UE 的移动性管理。GTP-C 协议在 IP 传输层之上运行,而 MAP 协议既可运行在 ATM 层之上,也可以运行在 IP 传输层之上。

图 10.38 示出了各 PS 域网元在典型分组数据会话(如任意的 IMS 过程)中的 PS 用户平面协议栈。UE 和 GGSN 之间的用户 IPv6 分组流由 UTRAN 用户平面协议和 GTP-U 隧道协议实现。在 SRNC,GTP 隧道协议和 PDCP 以及用户平面 RLC 协议相互协作,使 IP 分组可以在 WCDMA 无线接口上传输。

在图 10.38 中,我们假设分组数据流利用了 WCDMA 无线传输的 HSDPA 增强版。因此 MAC-d 消息通过高速下行链路信道帧协议(HS-DSCH-FP 或缩写为 HS-FP)从 SRNC 传输到 BS 基站。在基站处,实际的高速信道在 Uu 接口上,由 MAC-hs 协议维护。

在 PS CN 端,GTP 信道利用了在 Iu 和 CN 接口中的 IP 传输,根据 IMS 所选择的 IP 传输栈在 Gi 接口上传输。

10.7 IMS 协议总述

本节简述了 IMS 使用的主要协议,并列举出它们在不同参考点上的用处。在本书写作之时,R6 的工作仍然还在进行中,因此表 10.3 只可能总结现有的 IMS 参考点并列举相关的协议。

表 10.3 IMS 参考点总结

参考点名称	涉及的实体	目的	协议
Gm	UE、P-CSCF	该参考点用于在 UE 和 CSCF 之间交换信息	SIP
Mw	P-CSCF、I-CSCF、S-CSCF	该参考点用于在 SCSF 之间交换信息	SIP
ISC	S-CSCF、I-CSCF、AS	该参考点用于在 CSCF 和 AS 之间交换信息	SIP
Cx	I-CSCF、S-CSCF、HSS	该参考点用于 I-CSCF/S-CSCF 和 HSS 之间通信	Diameter
Dx	I-CSCF、S-CSCF、SLF	该参考点被 I-CSCF/S-CSCF 用于在一个多 HSS 环境下查找正确的 HSS	Diameter
Sh	SIP AS、OSA SCS、HSS	该参考点用于在 SIP AS、OSA SCS 和 HSS 之间交换信息	Diameter
Si	IMS-SF、HSS	该参考点用于在 IMS-SF 和 HSS 之间交换信息	MAP

（续）

参考点名称	涉及的实体	目　　的	协　议
Dh	SIP AS、OSA、SCF、IMS-SF、HSS	该参考点被 AS 用于在一个多 HSS 环境下查找正确的 HSS	Diameter
Mm	I-CSCF、S-CSCF、外部 IP 网络	该参考点将用于在 IMS 和外部 IP 网络之间交换消息	未说明
Mg	MGCF→I-CSCF	MGCF 把 ISUP 信令转化为 SIP 信令并且将 SIP 信令转换为 I-CSCF	SIP
Mi	S-CSCF→BGCF	该参考点 SIP 用于在 S-CSCF 和 BGCF 之间交换消息	SIP
Mj	BGCF→MGCF	该参考点 SIP 用于在相同的 IMS 网络中的 BGCF 和 MGCF 之间交换消息	SIP
Mk	BGCF→BGCF	该参考点 SIP 用于在不同的 IMS 网络和 BGCF 之间交换消息	SIP
Mr	S-CSCF、MRFC	该参考点 SIP 用于在 S-CSCF 和 MRFC 之间交换消息	SIP
Mp	MRFC、MRFP	该参考点 SIP 用于在 MRFC 和 MRFP 之间交换消息	H. 248
Mn	MGCF、IMS-MGW	该参考点允许对用户平面资源的控制	H. 248
Ut	UE、AS（SIP AS、OSA SCS、IMS-SF）	该参考点能够使 UE 管理与其自身或其服务相关的信息	HTTP
Go	PDF、GGSN	该参考点允许运营商在用户平面控制 QoS 并在 IMS 和 GPRS 网络之间交换计费的相关信息	COPS
Gq	P-CSCF、PDF	该参考点用来在 P-CSCF 和 PDF 之间交换策略决定的相关信息	Diameter
Ro	AS、MRCF、S-CSCF、OCS	该参考点被 AS、MRFC、S-CSCF 用于指向 OCS 的在线计费，注意，在 S-CSCF 和 OCS 之间可能存在一个相互作用的功能	Diameter
Rf	P-CSCF、S-CSCF、I-CSCF、BGCF、MGCF、AS、MRFC、CCF	该参考点被 IMS 功能用于指向 CCF 的离线计费	Diameter

3GPP 使用单一的 SIP（会话控制协议），该协议由 RFC 3261 定义。SIP 是一个应用层协议，在 IP 网络中，它用来建立、修改和结束多媒体会话。SIP 也是多媒体结构中的一部分，该结构的协议还处在由 IETF 进行标准化的阶段，其应用包括语音、视频、游戏、信息、呼叫控制和会议，但是不局限于这些。仅基本的 SIP 协议并不能满足 IMS 系统的操作，IMS 需要许多其他与 SIP 相关的 RFC（2327、3262、3264、3265、3311、3312、3313、3325、3327 等）请求的支持。如果要了解更详细的介绍，请参看 3GPP TS 24. 229 或 Poikselka 等的著作（2004 年）。

出于数据库查询和收费的考虑，也需要一个非 SIP 协议。当 IMS 实体需要与 HSS 或计费实体进行通信时，3GPP 选择使用 Diameter。

Diameter 是由 IETF 开发的认证、授权和计费协议（AAA 协议），它为多种接入技术提供 AAA 服务。Diameter 并不是直接起草建立起来的，而是从用户服务中 RADIUS（远程授权拨号）的建立思想中借鉴而来的，RADIUS 定义在 RFC 2865 中，用在拨号和终端业务接入环境中。Diameter 实际上包括一种能与 RADIUS 后向兼容的模式。

Diameter 实际可分为两部分：Diameter 基础协议和 Diameter 应用。基础协议用来传送 Diameter 数据单元、协商功能、处理错误和提供可扩展性。

Diameter 应用定义了与具体应用相关的功能和数据单元，每一个 Diameter 应用都是单独规定的。目前，除了 RFC 3588 定义的基础协议以外，还有一些已经定义的 Diameter 协议和一些正要定义的 Diameter 协议。此外，在 RFC 3539 中定义的 AAA 传输业务文档中还包括对 AAA 传输协议的利用所进行的讨论和建议，3GPP R5 也分配到了一个具体的 Diameter 命令代码集（定义在 RFC 3589 中）。

Diameter 基础协议使用 TCP 和 SCTP 作为传输协议，不过由于 Diameter 对等体之间存在面向连接的关系，更倾向于使用 SCTP。IPSec（IP 安全）（RFC 2401）和 TLS（传输层安全）（RFC 2246）都用于保护这些连接。

由于任何一个 Diameter 对等体都可以发起请求，使得 Diameter 是一个端到端的协议。Diameter 有三种不同类型的网络节点：客户端、服务器和代理。客户端一般是一个执行接入控制的网络边缘设备。Diameter 代理提供中继、代发、改向、转换等业务。Diameter 服务器为特定区域处理 AAA 请求。对 Diameter 消息的选路按照特定用户的 NAI（网络接入识别码）（RFC 2486）进行。Diameter 消息由 Diameter 头和其后的一些 Diameter AVP（Attribute Value Pair）构成。Diameter 头是用二进制表示的，这和 AP 头或 TCP 头类似（见图 10.39）。



图 10.39 Diameter 头结构

AVP 包含了封装好的 AAA 信息单元、路由单元、安全单元以及确认单元，这些都和特定的 Diameter 请求和应答消息有关。

在 3GPP IMS 中，Diameter 用于在参考点 Cx、Dx、Sh 和 Dh 进行定位和业务管理、用户数据处理、用户认证和授权，也用于在参考点 Rf 和 Ro 进行在线或离线计费。

出于 IP 策略控制目的，采用了 COPS（公用开放策略服务）（RFC 2748）。COPS 是一个用于对策略进行通用管理、确认和升级的 IETF 协议。它为策略服务器（如 PDF）和客户（GGSN）之间的策略信息交换定义了一个简单的问询/应答协议。在 PDF 和 GGSN 之间的参考点用 COPS 来执行媒体认证和计费收集，也用于策略扩展（RFC 3048）。此外，3GPP 还定义了个策略信息库，能识别策略提供数据。为了传送 IMS 策略控制数据，3GPP 已经定义了它自己的策略信息库，详见 3GPP TS29.207。

表 10.3 简单示出了 IMS 结构。为了简洁，表中不可能包括所有的内容，注意没有列出的内容如下。

- 计费相关的功能或参考点。
- 不同类型的 AS（应用服务器）。
- 不同 IMS 网络和 AS 之间的用户平面连接。

图 10.40 给出了带有参考点的 IMS 系统结构。但为了简明，略去了以下一些细节。

- 图中未示出 Mm、Mk、Mw 参考点的 SEG。
- 实体之间的虚线代表直接连接。
- ISC、Cx、Dx、Mm、Mw 在 S-SCCF 和 I-CSCF 处终止。

图 10.40 IMS 结构

第 11 章 处理过程实例

为了使读者能对前面所讲的 UMTS 系统中最重要的一些原理和功能有一个全网的概念，本章将给出一些 UMTS 系统处理过程的实例，这些处理过程实例示出了网络实体之间的协作方式以及 UMTS 协议所起的作用。

11.1 基本处理过程

本章将每一个系统过程视为一种通信事务，对系统范围的过程给出基本的模型。事务这一概念强调了整个系统的处理过程都能够准确实现，并且后面的每个处理过程都是一些独立的通信实例。

在第 10 章已经阐述了网络的层次结构，按层可以把整个网络划分为一系列不同的基本处理过程，每一个基本处理过程，在网络事务处理设计实现的时候，都可以作为一个封装模块进行处理。根据事务及其类型（如移动台主叫或被叫），基本处理过程中的一些消息和参数配置是变化的，而且有些基本处理过程可能不一定用到。

UMTS 协议互通模型（如图 10.4 所示）在此处的用处是，不同的处理过程使用 UMTS 网络的不同层。每一个处理过程中都需要用到传输网络：传输信令信息总是必需的，许多事务也需要传输数据业务。当基本处理过程需要执行接入网业务功能时就要使用无线网络功能。系统事务处理的整体控制由系统网络协议负责，它包含如何按步骤实行基本处理过程功能并且在不同的步骤中如何进行事务处理。

从原理上来说任何一个事务处理都可以分为 8 个步骤，如图 11.1 所示，每一个步骤区分出一个基本处理过程。

寻呼是一种移动性管理过程，它用来在网络覆盖区域中搜寻某一特定用户。该处理过程只有当事务由网络端发起时才会执行。其余 7 个步骤与事务是由 UE 发起还是由 UE 终止无关。

RRC（Radio Resource Control，无线资源控制）连接建立是一个基本处理过程，它包含了用于在移动终端和 RAN 之间建立无线控制连接所需的活动和信令流。该过程的细节与具体情形有关。

事务论证也是一个基本处理过程，在该处理过程中，移动终端告诉 CN（核心网）所请求事务的类型。CN 根据这一信息决定是继续还是终止事务的进行。

此后是鉴权和安全处理过程，该基本处理过程的目的是对 UMTS 的用户和网络进行互鉴权，接下来启动接入网连接所必需的安全机制。

事务建立和 RAB（无线资源业务）分配是一个为事务实际分配无线资源的基本处理过程，因此其细节与事务类型（电路交换还是分组交换）有关。

"事务"这个基本处理过程是存在用户平面连接（即 UE 有一个 UMTS 承载在整个 UMTS 网络激活）的阶段。

基本处理过程"事务处理清除和 RAB 释放"用于释放和事务处理有关的网络资源。

基本处理过程"RRC 连接释放"包含一些机制，这些机制用于释放 UE 和接入网之间的无线控制连接。



图 11.1　UMTS 网络事务处理基本模型

11.1.1　寻呼

寻呼用于执行到达 UE 的事务。与 GSM 系统不同，UMTS 定义了两种寻呼方法，分别称为寻呼方法 1 和寻呼方法 2。核心网采用寻呼方法 1，这是传统的寻呼方法，如图 11.2 所示。寻呼是无线网络控制平面的一部分，它使用 RANAP 寻呼消息在 Iu 接口上发送。发起寻呼的 CN 域寻址到 UE 通过位置更新或路由区更新最新报告的 LA/RA。

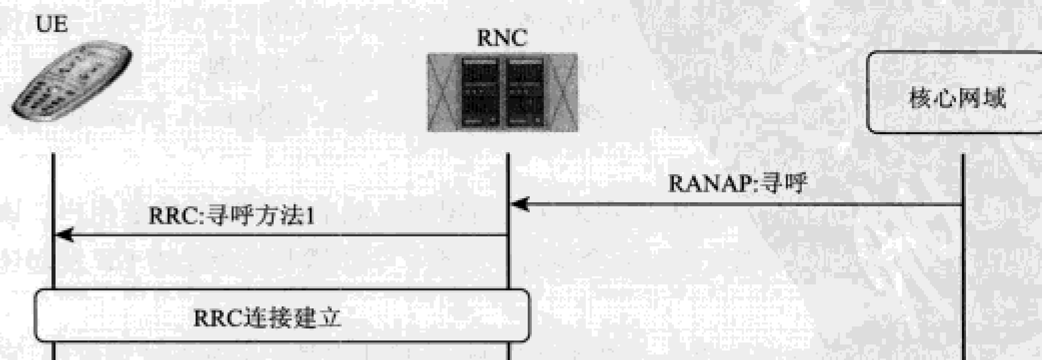


图 11.2　寻呼方法 1

RANAP 寻呼消息必须包含两个参数：提出请求的 CN 域以及国际移动台识别码 IMSI。从系统安全角度来看，不希望在 Uu 参考点处进行没有必要的未加密 IMSI 传输，因此，RNC 可能会对 IMSI 进行一些转换。例如，RNC 可能在 RRC 寻呼方法 1 消息中采用 RNTI（无线网络临时识别码）而不是 IMSI。RNTI 在 UE 连接到网络时或者在先前的事务中设置。

一般来说，UE 接收并识别出 RRC 寻呼方法 1 消息将会触发一个 RRC 连接的建立，该连接建立对于执行寻呼发起的事务是必须的。此外，RRC 寻呼方法 1 还有一些针对 RAN 的用途。若 UE 处于非空闲状态，而有些系统参数的改变需要让 UE 知道时，RNC 就可以使用寻呼方法 1 来唤醒 UE，使 UE 能够更新全部或者部分信息。如果 UE 有一个未活动的分组交换连接，RNC 用寻呼方法 1 来通知 UE 重新激活分组交换连接。此时 CN 会有一些分组数据信息需要传递给 UE，这将迫使 UE 执行小区更新操作，此后 RNC 便能把数据包路由到正确的 UE。

UMTS 的移动终端的设计使其可以同时处理各种连接，就是说在同一时间它可以有多个连接。当 UE 域已经和一个 CN 有一个连接时，建立到同一域的另一个连接时，CN 和原来一样发送 RANAP 寻呼。SRNC 发送的寻呼现在是用 RRC 寻呼方法 2（如图 11.3 所示）。

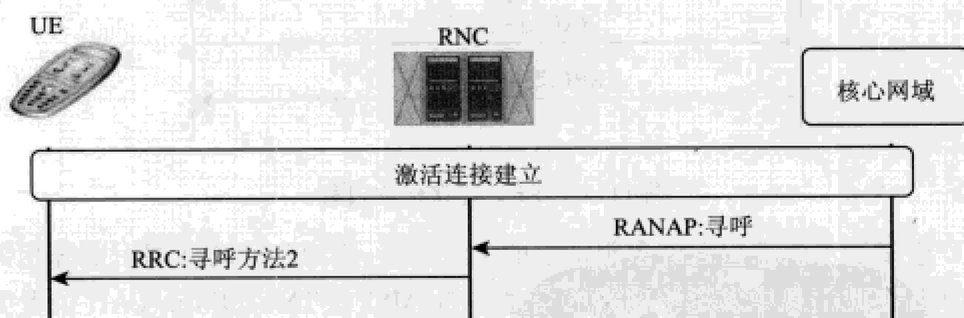


图 11.3　寻呼方法 2

在 RNC 中，RANAP 的形式总是一样的，寻呼方法 1 和寻呼方法 2 的区分由 RNC 进行。两者的差别在于：寻呼方法 1 寻呼的用户处于空闲状态、Cell-PCH 状态或者 URA-PCH 状态，因此它寻呼的目标可以是小区中的某一个用户或者小区中的所有用户。而寻呼方法 2 寻呼的用户总是处于 Cell-DCH 或者 Cell-FACH 状态，因此寻呼对象总是只有一个。

11.1.2　RRC 连接建立过程

图 11.4 示出了 UE 和 RNC 之间通过 Uu 接口和接入域内部接口 Iub 建立无线连接的原理。RRC 连接建立过程总是由 UE 通过 CCCH 发送 RRC CONNECTTION REQUEST 消息开始。如第 4 章所述，上行 CCCH 是 RACH（随机接入信道），因此 RRC CONNECTION REQUEST 实际是作为初始连接过程通过物理信道 RACH 进行传送的。

消息通过 Iub 的 RACH 数据端口到达 RNC，然后 RRC 实体将其状态从 IDLE 改变为 CONNECTED Cell_FACH 或者 Cell_DCH。此后 RNC 和 UE 通过公共控制信道（其中 FACH 和 RACH 分别使用）。

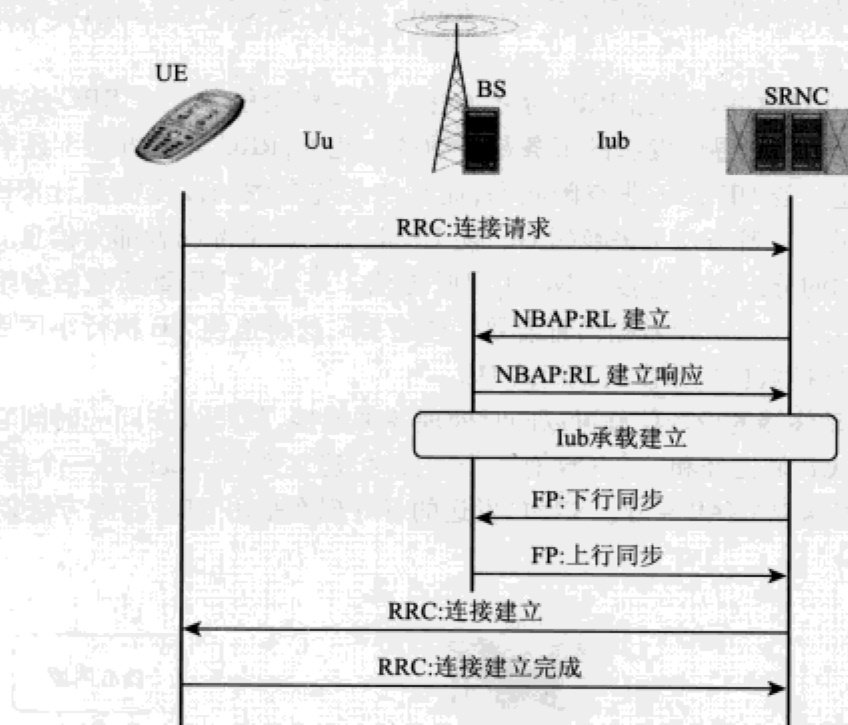


图 11.4　RRC 连接建立过程

RRC 连接请求消息包含许多跟请求的无线连接、用户和移动终端识别等相关的信息，以及 UE 在此消息中发送给网络的信息诸如 IMSI 或 TMSI、IMEI、LAI（位置区识别码）、RAI（路由区识别码）等。RRC 连接建立请求必须指示它包含了多少这样的信息以及它们的内容，另外还必须包含请求无线连接的原因。原因有很多，下面列出了一部分。

- 主叫对话业务呼叫。
- 主叫流业务呼叫。
- 主叫交互式业务呼叫。
- 主叫背景业务呼叫。
- 被叫对话业务呼叫。
- 被叫流业务呼叫。
- 被叫交互式业务呼叫。
- 被叫背景业务呼叫。
- 紧急呼叫。
- 高优先级信令。

- 低优先级信令。
- 重新建立呼叫。

可以看出,RRC 连接请求已经指示出了将要进行的事务的 QoS 要求。列出紧急呼叫是因为网络对它的处理方式和常规的通信不同。如果后续的事务只是信令,请求中也会显示。

RNC 根据连接请求的原因决定为事务分配公共资源专用资源。SRNC 再根据这样的决定分配 RNTI 和其他资源。RNC 向 BS 发送 NBAP RADIO LINK SETUP 消息时打开了 Iub 接口。这个消息包含传输格式描述、功率控制信息和码信息,码信息指 WCDMA-FDD 中的上行扰码。基站对此消息的确认应答是 NBAP PADIO LINK SETUP RESPONSE 消息,它向 RNC 通知有关传输层的地址信息(AAL2 地址),并为传输网建立 Iub 承载提供参考信息。

SRNC 根据从基站接收到的信息启动 Iub 承载的建立过程,该过程由 Iub 接口处的传输网络内部的控制层执行。所建立的 Iub 承载和分配给该事务的 DCH 绑定在一起。然后 Iub 接口处的帧协议连接与消息交换相同步。若使用 DCH 的专用无线链路建立在这里,那么它就是 DCH-FP(IubDCH 帧协议)。Iub 通信就绪后,RNC 通过公共控制信道(这里是 FACH)发送 RRC 连接建立消息给 UE,SRNC 通过该消息通知 UE 有关传输格式、功率控制和码的信息,对于 WCDMA-FDD,这里的码指下行扰码。UE 发送 RRC CONNECTION SETUP COMPLETE 消息来确认 RRC 连接的建立。

11.1.3　事务论证

UE 在 RRC 连接建立后发送 RRC INITIAL DIRECT TRANSFER 消息,其载荷包括该事务从 UE 到网络的第一个系统网络消息,如图 11.5 所示。

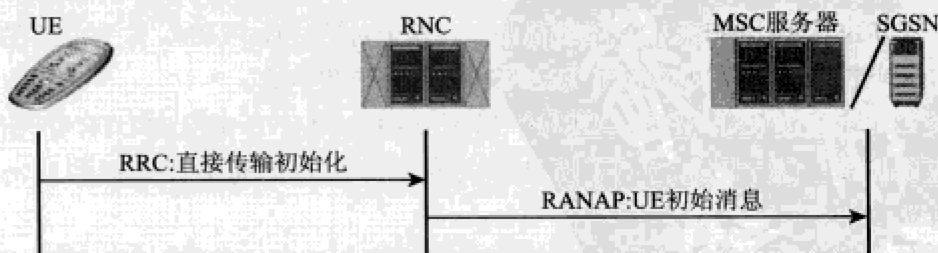


图 11.5　事务论证

RNC 收到消息后添加一些额外的参数,然后作为 RANAP UE INITIAL 消息转发给合适的 CN 域。RANAP UE INITIAL 消息包含了原来的 RRC INITIAL DIRECT TRANSFER 消息,以及 UE 产生的第一个系统网络消息。RANAP UE INITIAL 为 CN 提供了许多由 UE 初始化的事务的信息,包括声称的 UMTS 用户的识别码(TMSI 和 IMSI)、当前的位置区域以及所请求的事务类型。CN 节点(MSC/VLR 或者 SGSN)通过这些信息来决定如何处理事务处理请求。

11.1.4　鉴权和安全控制

在第 9 章中我们讨论了安全功能和算法，图 11.6 所示为一次事务过程中与接入网安全相关的信息流。

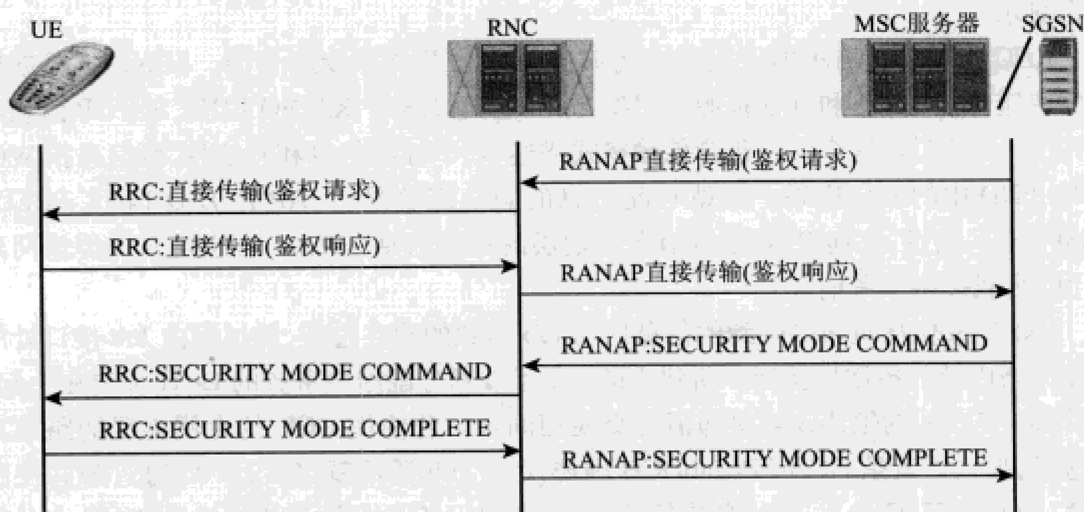


图 11.6　鉴权和安全控制处理过程

在 RRC 连接建立时 RNC 已经可以通过类别参数了解到 UE 的主要功能，其中之一就是 UE 支持的安全算法。

UE 和网络通过发送 MM AUTHENTICATION REQUEST 消息来相互鉴权，该消息包含在发送给 UE 的 RANAP AND RRC DIRECT TRANSFER 消息的载荷中。对 USIM 执行了鉴权算法之后，UE 用 MM AUTHENTICATION RESPONSE 消息做出响应，仍然是在 RANAP AND RRC DIRECT TRNSFER 消息的载荷中。在这个对话过程中，RNC 作为中继在 RANAP DIRECT TRNSFER 和 RNC DIRECT TRANSFER 之间转发内容。

相关 CN 域通过 RANAP SECURITY MODE COMMAND 消息向 UTRAN 指示该事务是否应该加密。这个消息指示了所选择的安全算法并把完整性密钥和加密密钥发给 UTRAN。

基于以上信息，RNC 通过发送 RRC SECURITY MODE COMMAND 要求 UE 用相应的密钥和算法开始加密。UE 通过发送 RRC SECURITY MODE COMPLETE 消息表示它已经成功转到所选的完整性保护算法和加密算法，从而可以保护该事务后续的通信。

RNC 还需向相关的 CN 域发送 RANAP SECURITY MODE COMPLETE 消息以表明这个过程已经结束。

11.1.5　采用无线接入承载分配的事务建立

到我们目前的讨论为止，基本处理过程都是相似的，因此都和 CN 域无直接关系。

从采用 RAB 分配的事务建立开始，就需要考虑和 CN 域的不同特性。

CS 事务建立的信息实际是通过 RRC/RANAP DIRECT TRANSFER 消息发送的，其载荷可以包含 CC SETUP 消息，如图 11.7 所示。该消息用于标识该事务并指示 QoS 要求，即业务所需要的承载类型，其参数应包括以下内容。

- TI(Transaction Identifier，事务标识)。
- 流标识。
- 业务类型。
- 非对称指示。
- 最大比特速率。
- 保证的比特速率。

UE 和 CN 节点借助 TI 区别各自的呼叫，每个呼叫都有自己的 TI 值。流标识识别呼叫所用的承载。如果没有流标识，表明 UE 端的 CC 协议希望建立一个新的承载。CC 协议希望建立多重呼叫时流标识也有可能已经存在，此时是通过该流标识所给定的承载来建立多重呼叫。

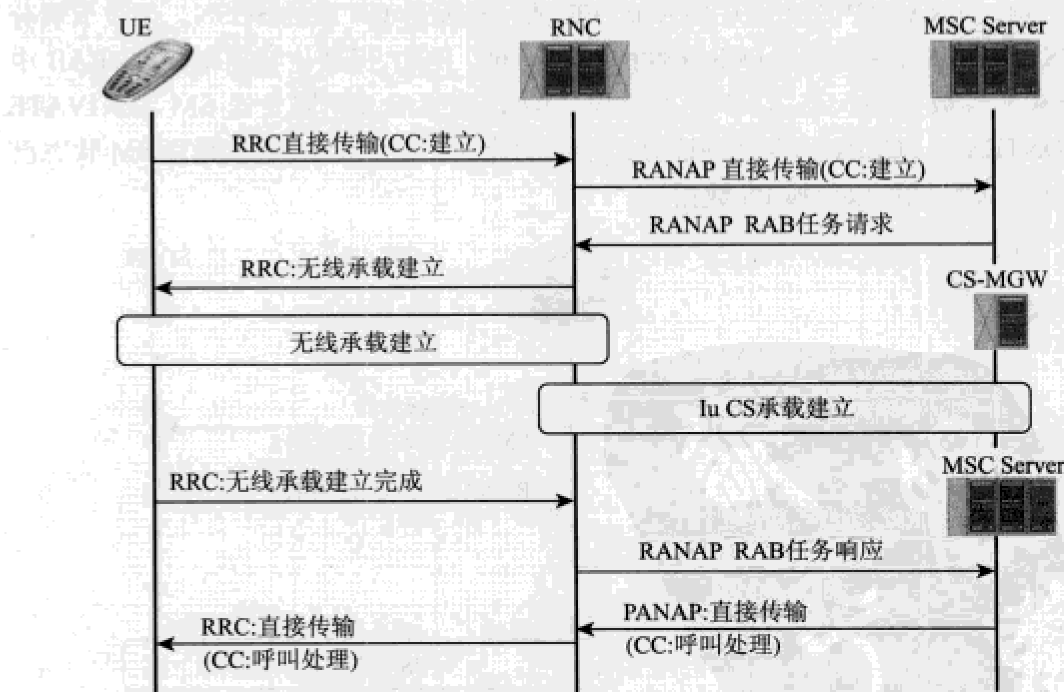


图 11.7 采用 RAB 分配的事务建立(电路交换)

接收到 CC SETUP 消息后，MSC 服务器开始工作。它先检查所请求的操作对 UE 及其当前的用户信息是否是允许的。如果允许的话，MSC 服务器开始 RAB 分配，它通过在 Iu 接口上发送 RANAP RAB ASSIGNMENT REQUEST 消息来分配唯一的 RAB ID 并请求建立满足 QoS 参数要求的 RAB。

RNC 在接收到 RANAP RAB ASSIGNMENT REQUEST 请求后，开始无线承载分

配。它先检查是否有足够的无线资源来满足所请求的 QoS。如果是,则根据请求分配无线承载。否则,RNC 将可能按较低 QoS 继续分配(例如可能降低承载的最大比特速率)或者排队等候资源。这些特殊情形需要一些图 11.7 之外的信令。

RNC 通过发送 RRC RADIO BEARER SETUP 消息向 UE 通知承载分配情况。UE 接收到这个消息后,结合最初发给网络的 CC SETUP 消息中的信息和收到的无线承载标识,就可以在正确的无线承载上发送用户平面业务数据。一旦 UE 能够从新的无线承载中接收数据,它将向 RRC 发送 RRC RADIO BEARER SETUP COMPLETE 消息作为确认应答。RNC 还必须要为新的事务建立一个 Iu 承载。然后,RNC 向 MSC 服务器发送 RANAP RAB ASSIGNMENT RESPONSE 消息以表明 RAB 已分配。如果 RNC 对 MSC 服务器请求的 QoS 有变动,也将表示在这个消息中。至此,RAB 已经建立,过程继续在 CC 协议层进行。

如果是为 PS 事务建立 RAB,过程基本类似(如图 11.8 所示),差别主要在消息上。UE 现在用 SM(Session Management,会话管理)协议来替代 CC 协议。UE 向网络发送 SM ACTIVATE PDP CONTEXT REQUEST 消息作为 RRC DIRECT TRANSFER 消息,RNC 将其作为 RANAP DIRECT TRANSFER 消息转发给 CN 域的 SGSN。无线承载分配和 CS 业务类似,只是描述 QoS 属性的参数不同。例如,保证比特速率在 PS RAB 中是一个基本参数,但对 CS RAB 并不重要。RAB 建立后 CN 域发送 SM ACTIVATE PDP CONTEXTACCEPT 消息来确证分组会话的建立。在 SM 中,这就是说 SM 状态已激活,UE 和 CN 域可以交换 PS 数据。

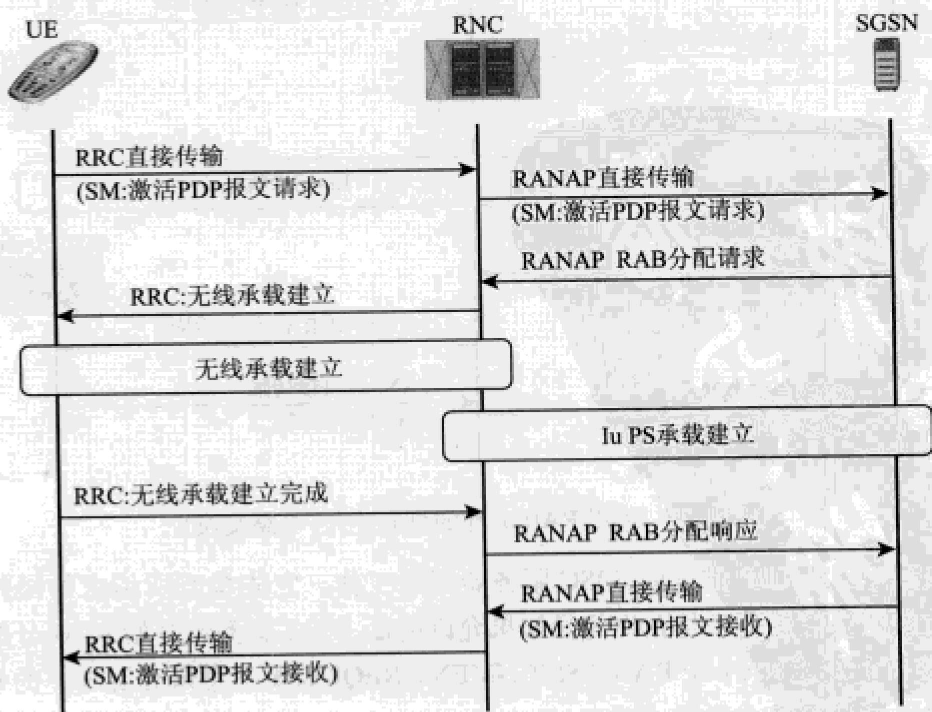


图 11.8 采用 RAB 分配的事务建立(PS)

11.1.6 事务

绝大部分情况下，事务的这个阶段有一个激活的用户平面连接。本章稍后将给出这种事务的具体实例（见 11.4 节）。但若 RRC 连接请求纯粹是为了信令（例如 MM 活动），就不需要用户平面承载，而是用一个信令连接来执行 MM 活动（见 11.3.3节的例子）。

11.1.7 事务清除和 RAB 释放

如果事务有激活的用户平面，则先断开用户平面。断开的过程与事务类型有关。图 11.9 示出了 CS 事务的清除。在图 11.9 中，清除由 UE 启动，但 CN 也可以启动断开用户平面。通常来说，无论哪一方是主叫，任何一方都可以清除常规的 CS 呼叫。

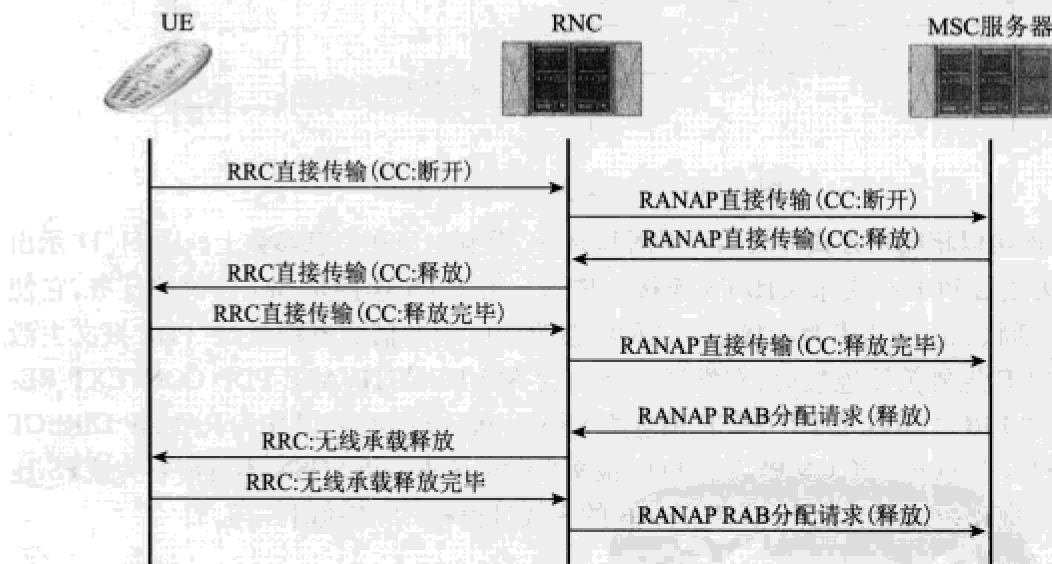


图 11.9 CS 事务清除信令及 RAB 释放

用户平面断开后，系统通过单独的子过程来释放 RAB。如果是用 RANAP RABASSIGNMSNT REQUEST 和 RANAP RAB ASSIGNMENT RESPONSE 消息，就是图 11.9 所示的情形，此时仍然保持信令连接。UE 仍然有到 UTRAN 的 RRC 连接，该 UE 的其他 RAB 继续存在。一般来说，只有一个 RANAP RAB 分配请求消息时，CN 可以生成、删除和修改多个 RAB。

如果要同时释放 UE 和 CN 域之间的所有 RAB 并收回相关的无线资源，可以用 RANAPIU RELEASE 命令，如图 11.10 所示。收到该命令后，RNC 在 Iub 接口启动 RRC RADIO BEARER RELEASE，此外还释放所有通过 DRNC（漂移 RNC）建立的无线承载。无线承载释放后，RRC 连接也释放。所有无线承载和 RRC 连接都释放完后，RNC 向 CN 域发送 RANAP IU RELEASE COMPLETE 消息。

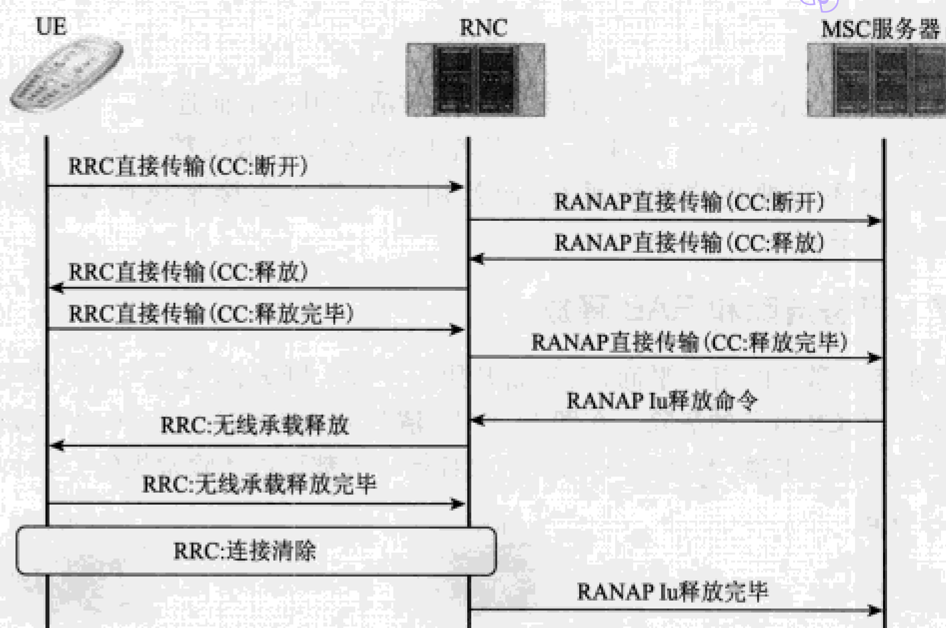


图 11.10　CS 事务清除和 Iu 释放

PS 连接以相同的方式释放用户平面和 RAB,差别也只在消息参数上。图 11.11 示出了通过去激活 PDP 报文来关闭 PS 连接的情形。关闭 PS 连接是 SM 协议的任务,它使 SM 从激活状态改变为未激活状态。这种状态改变所用的信令过程就是“PDP 报文去激活”。当 UE 想要关闭连接时,它发送一条包含 SM DEACTIVATE PDP CONTEXT REQUEST 的 RRC DIRECT TRNSFER 消息给 SRNC,然后 SRNC 将其作为 RANAP DIRECT TRANSFER 消息转发给 CN PS 域。PDP 报文去激活请求告诉 SGSN 不再需要为该 PS 连接所分配的 RAB,因此应当释放掉。RAB 的释放过程和 CS 连接时一样。

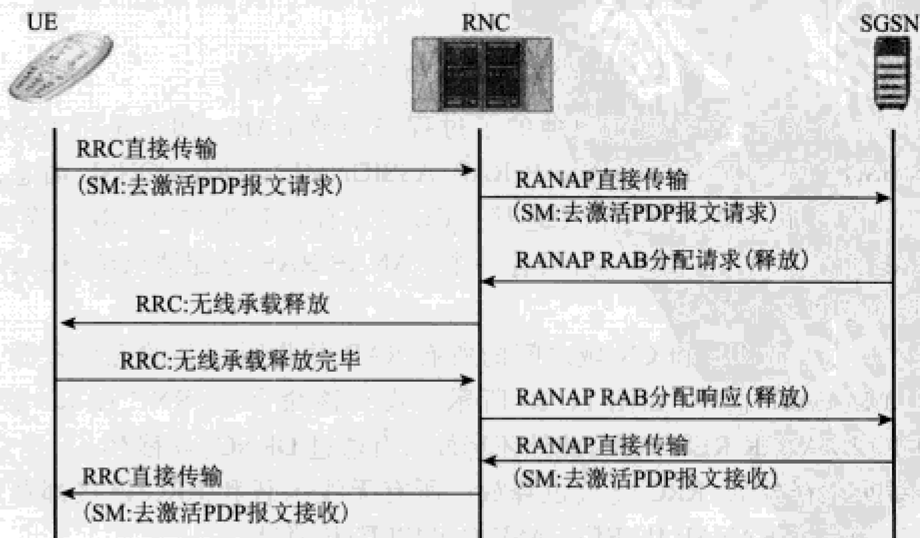


图 11.11　PS 事务清除和 RAB 释放

RAB 释放后,SGSN 向 UE 发送 SM DEACTIVATE PDP CONTEXT ACCEPT 消息,指示 PS 连接目前已经失效。此过程后,UE 和网络之间仍然有 RRC 连接,并可能有其他打开的 CS 和 PS 连接。如果要关闭所有的 PS 连接并收回相关的无线资源,系统也像 CS 连接时那样使用 RANAP IU RELEASE 命令,如图 11.12 所示。

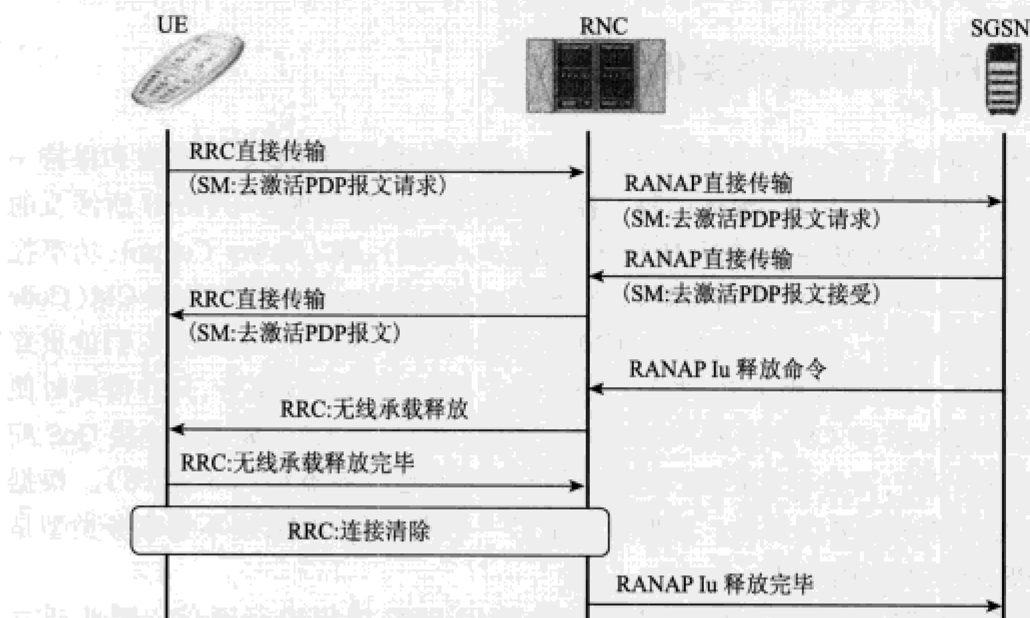


图 11.12　PS 事务清除和 RANAP Iu 释放

11.1.8　RRC 连接释放

RRC 连接释放过程如图 11.13 所示,该过程总是由 RNC 发起。RNC 识别出拟释放的 RRC 连接,再将此信息通过 RRC CONNECTION RELEASE 消息发送给 UE。UE 通过发送 RRC CONNECTION RELEASE COMPLETE 消息来确认该 RRC 连接已经释放。

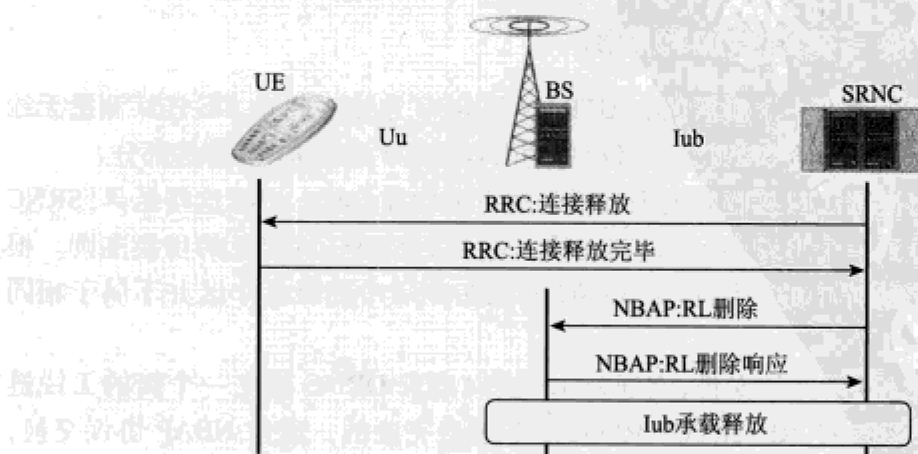


图 11.13　RRC 连接释放

此后，RNC 开始清除 Iub 接口的资源。这是通过交换 NBAP RADIO LINK DELETION 和 NBAP RADIO LINK DELETION RESPONSE 消息完成的。当无线链路删除在 NBAP 级相吻合时，Iub 接口处的传输数据承载就被释放。同时通过 Iur 子过程释放所有在 DRNC 上建立的无线链路（图 11.13 中未示出）。

11.2 RRM 处理过程实例

如第 5 章所述，RRM 是一系列算法的集合，用来在 RNC 和 UE 之间建立和保持一条质量好的无线路径。因此 RRM 的每一种算法基本上都会出现在 UTRAN 所涉及的所有事务中。RRM 算法主要包括 HO（Hand Over，切换）、PC（Power Control，功率控制）、AC（Admission Control，接纳控制）、PS（Packet Scheduling，分组调度）和 CM（Code Management，码管理）。其中 PC、AC 和 CM 是连续使用的，从事务一开始，它们就贯穿在各个阶段中。分组调度用于 PS 事务。切换用于 CS 和分组 PS 事务，只在需要时使用。因为在 UTRAN 中 CS 事务和 PS 事务是平等的，因此对切换的要求由连接 QoS 配置定义（见第 8 章），并且使用的是无线信道类型而不是事务类型（CS 或 PS）。根据 QoS 配置，实时事务需要用切换。若事务使用了一个或多个 DCH，则不管事务类型是 CS 还是 PS，都需要应用切换。

位于 UE 和 RNC 通信之间的 RRM 实体使用 RRC 协议进行通信。因此建立 11.2.2 节所述的 RRC 连接对每个事务都是必需的。不过需要注意的重要一点是，不管各种系统范围的事务同时打开了多少个无线承载，每个 UE 只需要一个到 UTRAN 的 RRC 连接。

本小节将给出一些切换的实例。先介绍软切换，其原理见第 5 章。然后概述 SRNS 重定位过程，这个过程不涉及 UE。最后给出的 RRM 处理过程实例是系统间切换，在该实例中，UE 执行从 WCDMA 到 GSM 无线接入的切换。

11.2.1 软切换－链路增加和删除

UE 使用业务时，存在一个激活的到 UTRAN 的 RRC 连接。此时，UE 连续测量无线连接并且把测量报告发送给 SRNC。测量报告的内容见第 5 章的 RRM 算法部分。

SRNC 中的切换算法对接收到的测量报告进行平均和分析。根据这些结果，SRNC 发现 UE 已经测量到一个 BS2 的小区，其无线条件满足 SRNC 所定义的切换准则。根据存储在 SRNC 数据库中的网络信息，SRNC 发现在 BS2 中的目标小区并不属于相同的 RNS。

SRNC 在 UTRAN 端开始安排，它通过 Iur 接口请求 DRNC 建立一个新的无线链路，这是通过发送 RNSAP RL SETUP REQUEST 消息完成的。通过 NBAP 协议交换，它触发 DRNC 以在 DRNC 和 BS 2 之间的 Iub 接口上建立一个无线链路。这些步骤之后，Iub 和 Iur 承载已建立，并且在 SRNC 和 BS 2 的下行和上行方向的帧协议也已经实

现了同步。Iub 和 Iur 接口处的帧协议实现无线网络的用户平面和加载用户数据流。在本实例中，我们假设所用业务是语音呼叫，因此所用的帧协议就是 Iub/Iur 的 DCH-FP。

SRNC 在 FP 上行同步后，发送一个 RRC ACTIVE SET UPDATE 消息给 UE，告诉它一个经由 BS 2 中小区的新无线链路已经添加到激活集中，并已可以使用。UE 发送 RRC ACTIVE SET UPDATE COMPLETE 消息作为确认应答。

从承载体系来看，这个实例中 UE 有一个激活的 CS RAB。该 RAB 的实现在 UTRAN 内是通过 SRNC 和 CN 之间的 Iu 承载，另一段是从 SRNC 经由 BS 1 的小区到 UE。从 QoS 和承载的角度来看，图 11.14 所示的过程是 SRNC 在已有连接的基础上增加了一个无线承载。RAB 和 Iu 承载保持不变。帧协议同步后，SRNC 把 RAB 映射到无线承载上。这种情形以及相关协议简单地示于图 5.35 中。

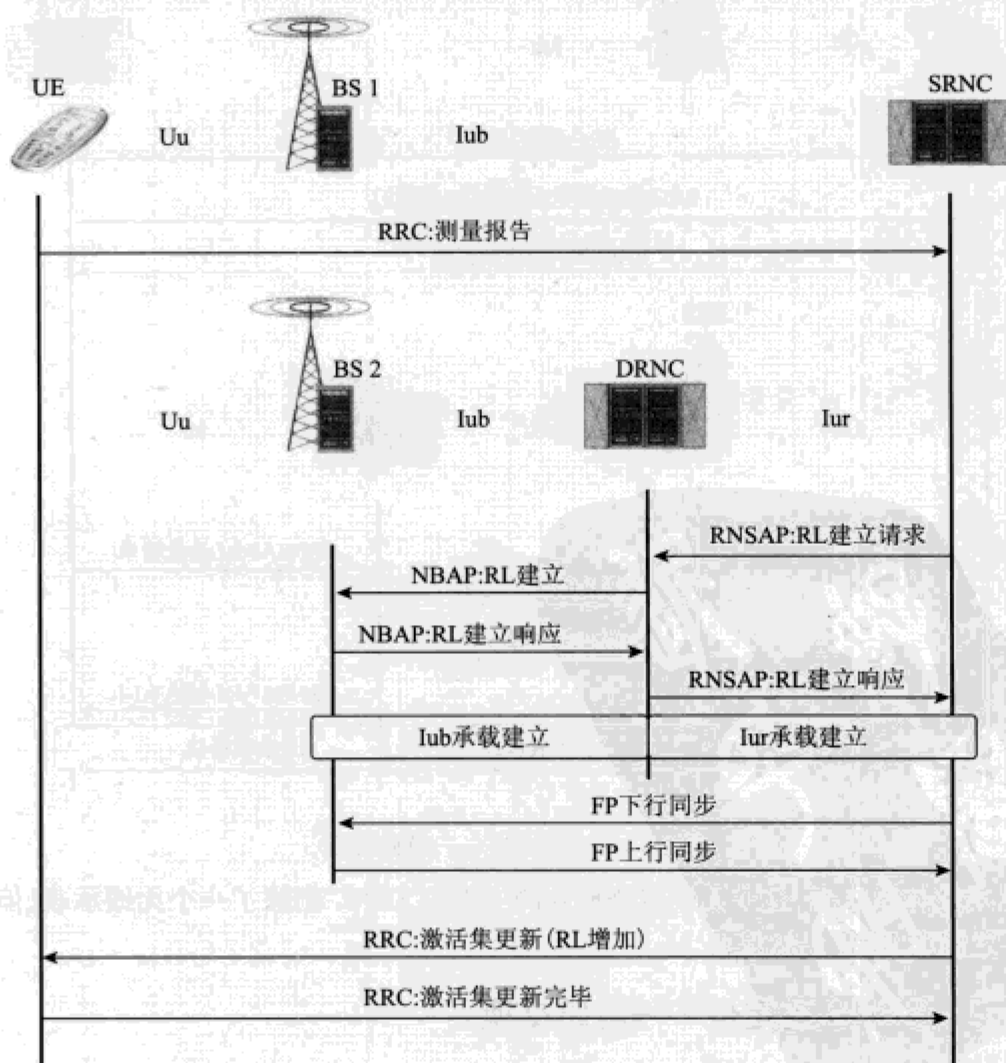


图 11.14 软切换——链路增加

当 UE 在事务期间在网络内移动时，会有这样一个时刻，SRNC 从测量报告发现通过 BS 2 的小区携带无线承载的无线连接不再符合要求。这时 SRNC 将会通知 UE 从激活集中删除这个无线链路，这也是通过发送 RRC ACTIVE SET UPDATE 消息来完成的。UE 向 SRNC 发送 RRC ACTIVE SET UPDATE COMPLETE 消息来确认无线连接的删除。

接收到 UE 发来的确认信息后，SRNC 开始删除它和 BS 2 之间的无线链路。此处使用 Iur 接口上的 RNSAP RL DELETION REQUEST 消息来完成，通过 NBAP 协议，该消息又触发 DRNC 来删除 Iub 接口上的无线链路，同时相关的 Iub 和 Iur 承载也被释放。软切换无线链路删除相关的消息流如图 11.15 所示。

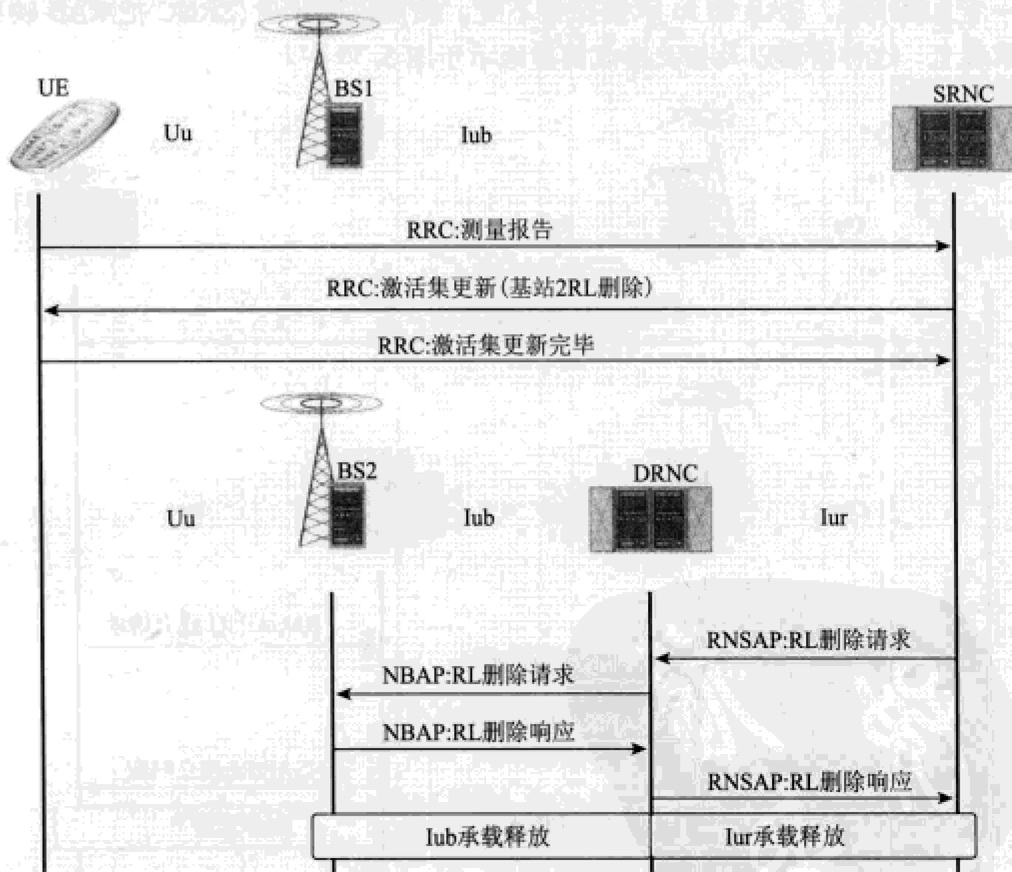


图 11.15　软切换——链路删除

从承载体系来看，这个无线链路删除的实例中 SRNC 删除了一个无线承载，但 CN 和 UE 之间的 RAB 仍然保留。

11.2.2　SRNS 重定位——电路交换

SRNC（Serving RNC，服务 RNC）的作用是为某一个激活的 UE 维护 Iu 承载并执行 RAB 到无线承载的映射。由于软切换（见 11.2.1 节）的原因，无线承载的无线链路组

成成分可能不断改变，所以可能出现这种情形，SRNC 并没有管理任何直接通过 Iub 接口到其基站的无线链路。此时，RAB 映射功能应当改到位置更好的 RNC。由于 RAB 映射要求在相同的 RNC 中有 Iu 承载，所以 CN 连接也将变更。

SRNS 重定位就是这样一种 RRM 过程，它把 Iu 承载的终点从一个 RNC 改变到另外一个 RNC，无线承载也同时改变。该过程的消息流如图 11.16 所示。图中 RNC 1 是原来的 SRNC，RNC 2 是将要采用的 RNC，将由它实现 SRNC 的功能。SRNS 重定位过程有两种实现方法：涉及 UE 或者不涉及。这里给出的是不涉及 UE 的实例。

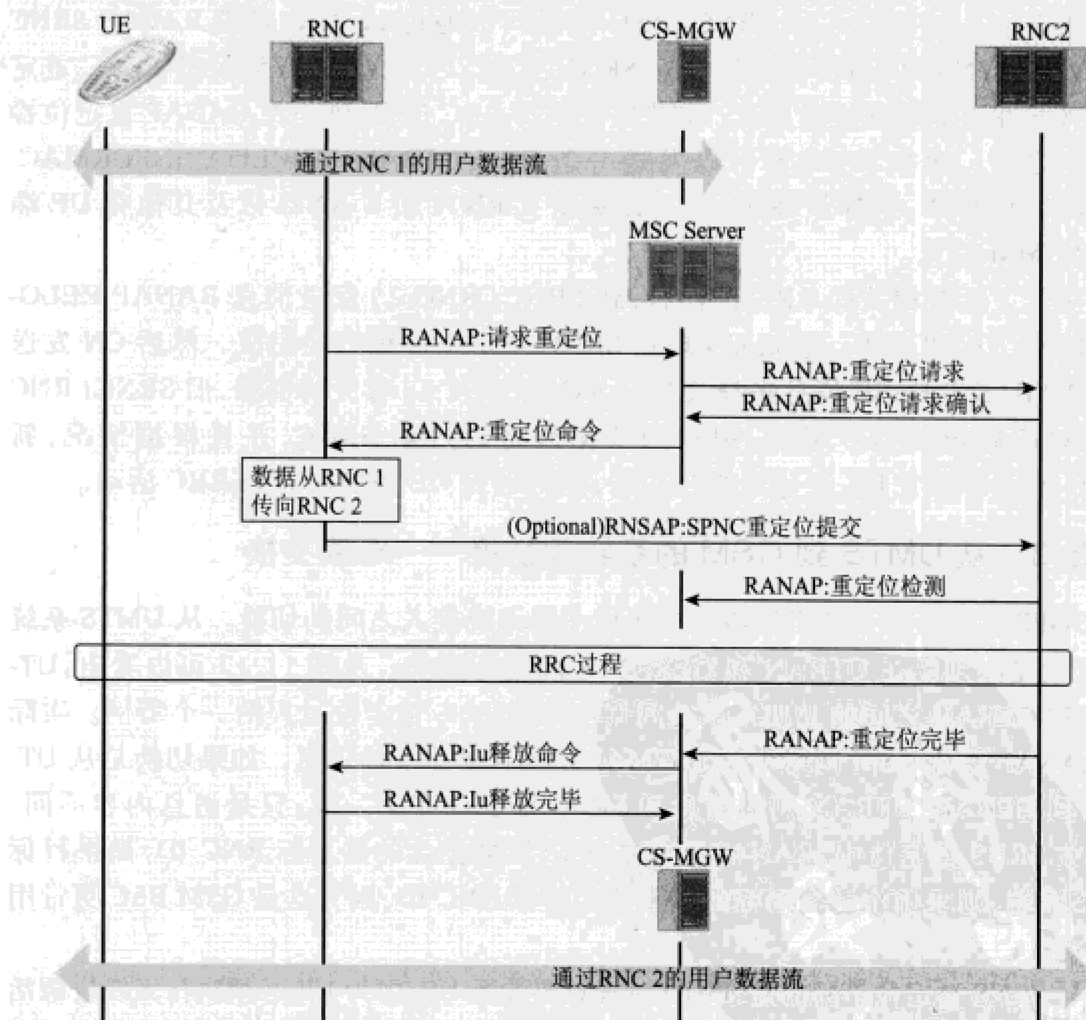


图 11.16　CS SRNS 重定位(不涉及 UE)

当原来的 SRNC(即 RNC 1)认识到 SRNC 功能应该转给更合适的 RNC (RNC 2)时，它通过 RAPAP RELOCATION REQUIRED 消息和相关的 CN 域进行联系，从而启动这个过程。该消息包含重定位的原因、目标 RNC 识别和 UE 类型等信息。CN 域根据目标 RNC 标识将这个请求转发到目标 RNC，转发用 RANAP RELOCATION REQUEST 消息。除了重定位相关的信息之外，RANAP RELOCATION REQUEST 消息还

包含了承载报文信息，CN 根据这些信息同时把 RAB 和 RRC 连接的终点从原来的 SRNC(即 RNC 1)转移到目标 SRNC(即 RNC 2)。

如果目标 RNC 有足够的资源来处理新到的 SRNC 功能，它将发确认信息给 CN，CN 再把确认信息转发给源 RNS。从 RNC 1 来看，该确认信息是启动重定位的命令，因为此时目标 RNC 已经就绪。接收到 RANAP RELOCATION COMMAND 后，原来的 SPNC(RNC 1)开始转发数据到目标 SRNC(RNC 2)。目标 SRNC(RNC 2)发现新来的数据后通过 RANAP RELOCATION DETECT 消息使 CN 域知道已检测到重定位。有些时候，原 SRNC(RNC 1)也可以通过 Iur 接口发送 RANAP SRNC RELOCATION COMMIT 消息给目标 SRNC(RNC 2)。在 UE 不涉及的 SRNC 重定位中，UE 并不知道这些消息流。如果需要执行 RRC 过程，则是在 RANAP 重定位检测消息之后。比如 UTRAN 可以发送一条 RRC UTRAN MIBILITY INFORMACTION 消息给 UE，这样 UTRAN 就可以更新 C-RNTI 和 U-RNTI 以及其他在 UE 端的相关 MM 信息。

执行了所有相关的 RRC 过程后，新 SRNC(RNC 2)发送消息 RANAP RELOCATION COMPLETE。通知 CN 现在 SRNC 重定位过程已经完成。然后 CN 发送 RANAP IU RELEASE 消息来释放和旧 SRNC(RNC 1)有关的资源，旧 SRNC(RNC 1)将对此做出确认。现在，用户的数据流将通过新 SRNC，并且根据情况，新 SRNC 还可以作为 UE 宏分集的合并点，同时也为 UE 控制所有的 RRC 活动。

11.2.3 从 UMTS 到 GSM 的系统间切换——电路交换

3GPP 标准要求系统必须能支持两种不同无线接入之间的切换。从 UMTS 系统来说，就是必须能在 UTRAN 和 GERAN 之间进行切换。从图 11.17 可以看出，UTRAN 和 GERAN 之间的 ISHO(系统间切换)是 SRNS 重定位过程的一个特例。实际上，RANAP 要比 GSM 网络中的 BSSMAP 协议包含更多的信息。如果切换是从 UTRAN 到 GERAN，UTRAN 侧的消息和 SRNS 重定位完全一样，只是消息内容不同。例如在 SRNS 重定位中，RANAP 重定位要求消息包含的是目标 RNC ID，如果目标在 GSM 端，则采用小区全局标识码来替代目标 RNC ID，因为这是 GSM BSC 更常用的标识。

与 SRNS 重定位不同的是，ISHO 过程总要涉及 UE，因为 UE 必须执行无线资源活动以接入 GERAN。注意 GERAN 不一定能处理所有对 UTRAN 有效的报文信息。UE 必须能测量 UTRAN 小区周围的 GSM 小区，UTRAN 是靠时隙模式来做到这一点的(见第5章)。时隙模式使 UE 能有一些时间来测量 GSM 频段，从而确定出候选的切换对象。有关这些切换对象的信息和测量报告也像 UTRAN 小区一样发送给 RNC。

当 RNC 发现 GSM 小区是最合适的选择，而且无其他 UTRAN 小区可用时，SRNC 向 CN 请求重定位信息。CN 检查 RANAP RELOCATION REQUIRED 消息，得知切换目标小区属于 GSM BSS。于是，CN 发送消息 GSM BSSMAP HANDOVER REQUIRED

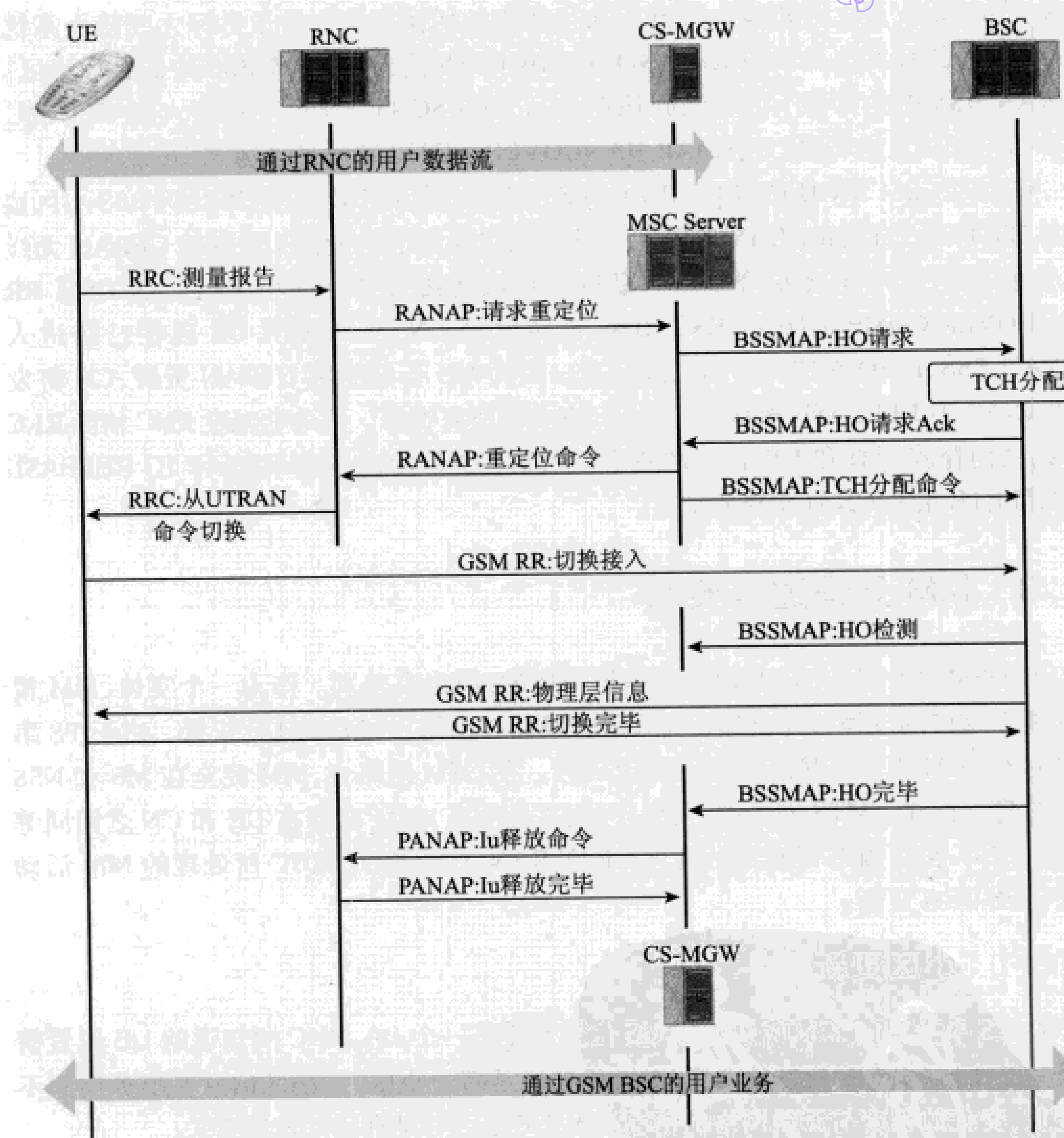


图 11.17 从 UTRAN 到 GERAN 的系统间切换——电路交换

给 GSM 网络的目标 BSC。该消息使目标 BSC 为该连接的切换建立 TCH(业务信道)。GERAN BSS 完成 TCH 分配后,返回确认消息给 CN,CN 把它作为 RANAP RELOCATION COMMAND 消息转发给 SRNC。

RANAP RELOCATIOM COMMAND 启动了 SRNC 中的重定位过程。由于这种情况涉及 UE,所以 SRNC 发送 RRC HANDOVER FROM UTRAN 来命令 UE 执行系统间切换功能。该切换命令包含目标系统的有关信息,并可能包含其他与系统间切换有关的信息。

UE 收到 RRC HANDOVER FROM UTRAN 命令后,检查命令是否指示了特定的

切换时间(默认是立即切换),并开始执行相应的切换操作。由于目标无线接入系统是 GERAN,UE 发送 GSM RR HANOVER ACCESS 消息给 GSM BSS 中的目标小区。GERAN BSS 中的目标小区检测到该信息后,向 BSC 指示 UE 正在接入到 GERAN。BSC 再向 CN 发送 GSM BSSMAP HANDOVER DETECT 消息来通知 UE 的到达。

作为对 GSM RR HANDOVER ACCESS 消息的确认,UE 将从 GERAN BSS 小区接收到 GSM RR PHYSICAL INFO 消息。该消息包含的信息能使 UE 启动 GERAN 无线接入(例如信道描述会发给 UE)。最后,UE 成功接入到目标小区后发送 GSM RR HANDOVER COMPLETE 给 BSC,BSC 再转发给 CN,从而表明 UE 现在已经进入 GERAN BSS,ISHO 在这一方面已经完成。因为 UE 不再使用 UTRAN 资源,CN 将发送 RANAP IU RELEASE 来释放和该 UE 有关的所有资源。该命令触发 RNC 清除 RRC 连接,从而释放所有和 UE 有关的资源。然后,RNC 发送消息 RANAP IU RELEASE COMPLETE 来向 CN 证实释放结束。

11.3 MM 处理过程实例

和 GSM 相比,UMTS 中 MM 很多是一样的,但也有差别。作为一个实体,MM 覆盖了所有这样的过程、方法和标识码,用来跟踪在网络中移动的 UE 位置。由于 PS 事务的存在,MM 引入了状态模型(见第 6 章)。在 GSM 网络中,MM 完全在 MS 和 NSS 之间处理。而在 UMTS 网络中,大部分(但不是所有)MM 功能在 UE 和 CN 之间同等处理。RNC 也用 RRC 过程部分处理 UE 在 RAN 中的移动。RNC 所处理的 MM 活动是小区及 URA 更新。

11.3.1 小区更新

在 CS 事务期间,CN 所知道的 UE 位置精度是一个 LA,RNC 所知道的 UE 位置精度是一个小区(若 UE 处在软切换,更准确地说是多个小区)。小区信息在事务期间不断变化,变化的程度与无线网络的情况以及 UE 是否移动和移动速度有关。

在 PS 事务位置信息的发布中,CN PS 域所知道的 UE 位置精度是 LA 及 RA,RNC 所知道的 UE 位置精度是小区。PS 连接本质上不是连续的,所以当 UE 和 CN 之间的数据连接暂时关闭时,RNC 中的小区可能会过时。因此,PS 连接是从 UE 和 CN 的角度来看的,但 RNC 不能以这样的方式路由分组数据。如果 UE 想发送数据包而当前小区和先前不同时,UE 将会执行 RRC 小区更新过程(如图 11.18 所示)来向 RNC 通知当前的小区。此后,任何 RRC 活动原则上都能运行(例如建立无线承载)。

另一方面,如果是 CN PS 域有分组数据需要传输给 UE,那么 CN PS 域首先发送 RANAP PAGING 消息使 RNC 发送 RRC PAGING TYPE I 消息给 UE。UE 接收到这个消息后,检查是否需要进行小区更新过程。如果需要,UE 就执行小区更新,然后就可以接收分组数据了。总的来说,有很多种情况需要 UE 执行小区更新,如下所示。

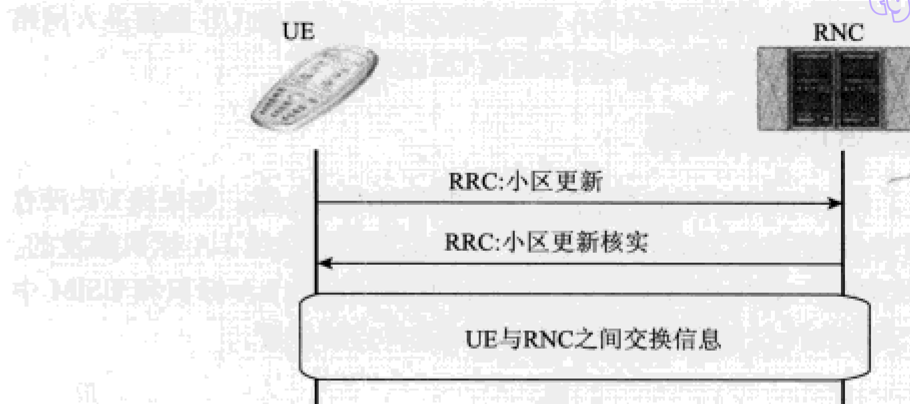


图 11.18 小区更新过程

- 小区重选。
- 定期小区更新。
- 上行数据传输。
- 寻呼响应。
- 重新进入服务区。
- 无线链路故障。
- 无法修复的 RLC 错误。

与小区更新过程相关,RNC 可能会给 RRC 连接分配一个新的 RNTI。

11.3.2 URA 更新

RNC 记录着每个 UE 当前的 URA。如第 6 章所述,URA 由许多小区组成,这些小区可能属于同一个 RNC,也可能分别属于不同的 RNC。URA 和 LA 和 RA 一样,是 UE 存储在 USIM 中的一个标识。UE 开机后不断监视接收到的 URA 标识。如果接收到的 URA 和存储在 USIM 中的不同,UE 就会执行 RRC URA 更新过程(如图 11.19 所示)。

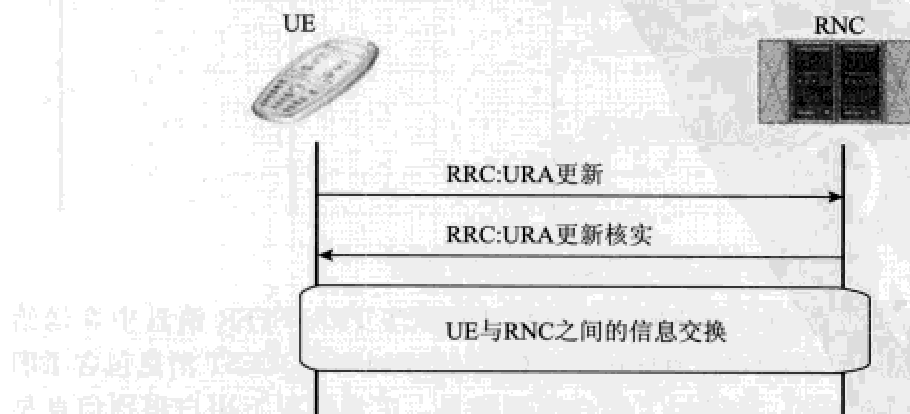


图 11.19 URA 更新过程

能触发URA更新的其他情形包括URA定期更新定时器到期和UE重新进入网络的服务区。和小区更新时一样，RNC将改变分配给UE的RNTI。

11.3.3　CN CS域的位置更新

图11.20示出了UE和CN CS域之间进行位置更新时的信令流。如果该UE没有和UTRAN的RRC连接，将先建立RRC连接。实际的位置更新是由LA标识触发的。UE把LA存储在USIM中，如果从系统信息中收到的驻留小区的LA标识和USIM中存储的不一样，UE开始执行位置更新过程以使CN知道其当前位置。

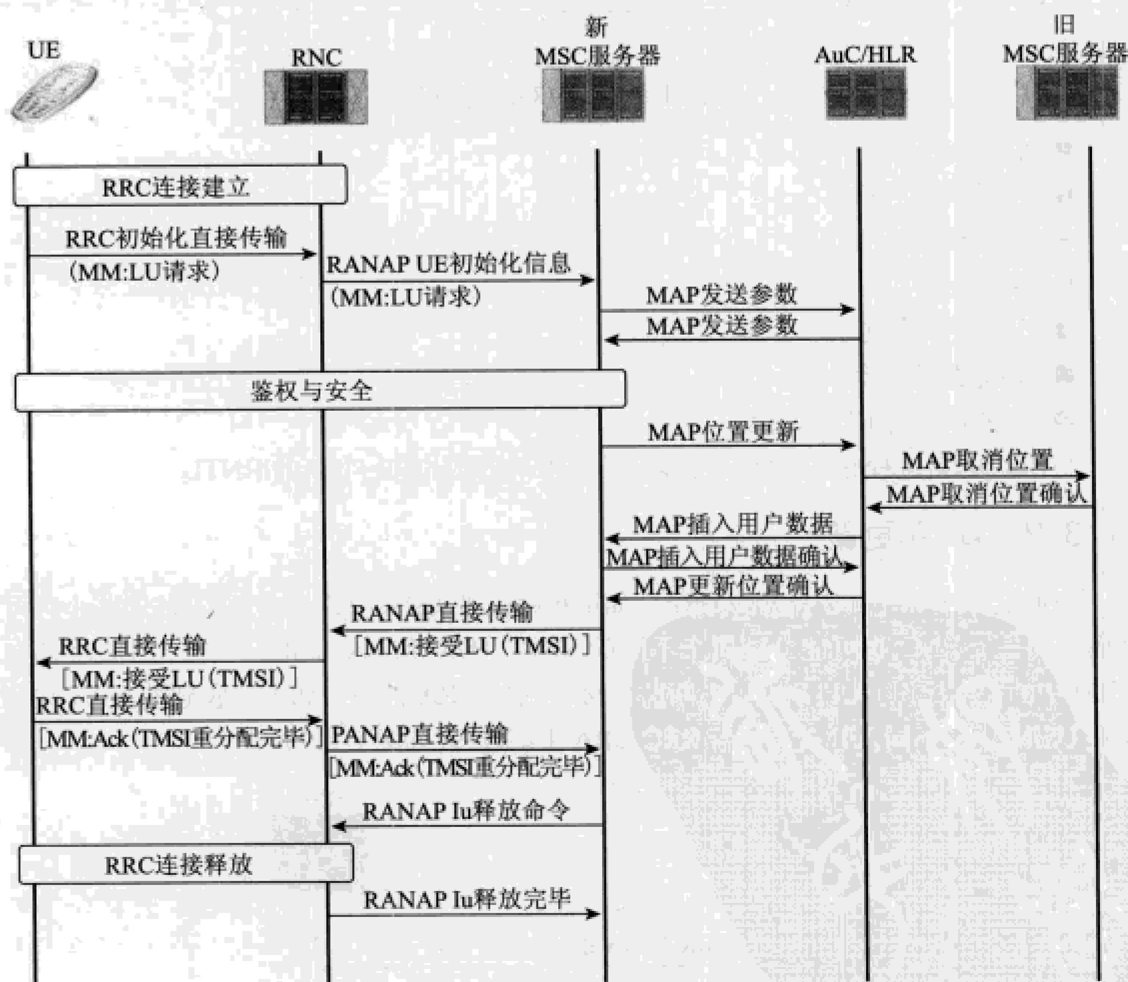


图11.20　CNCS域的位置更新

MM LU REQUEST消息装在RRC INITIAL DIRECT TRANSFER消息中发送给RNC，又通过RANAP UE INITIAL消息转发给CN。MM LU REQUEST消息包含了旧的LA标识和新的LA标识，并附加了用户识别信息。正常情况下用户识别信息是MSC服务器先前分配的TMSI。

在MSC服务器中的VLR功能判断它是否有该用户的鉴权向量。如果没有就从

AuC 中提取相应的安全参数，AuC 通过 MAP SEND PARAMETERS 消息发送预定的一些参数给 VLR。VLR 收到参数后即可启动接入级的安全过程以进行鉴权和加密。如果新旧 LA 标识不同，VLR 向用户的 HLR 通知新的位置。HLR 用 MAP CANCEL LOCATION 消息取消 UE 原来的位置信息，并开始 MAP INSERT USER DATA 操作。该操作把用户配置发送给新的 VLR。用户配置包含所有必要的标识、业务特性以及对该用户可能存在的使用限制。VLR 更新了用户的位置信息后，CN 域发送 MM LU ACCEPTED 来通知 UE 该过程完成。这个消息包含用户的新 TMSI。RNC 通过 RRC DIRECT TRANSFER 消息将这个信息转发给 UE，UE 向 MSC 服务器发送 MM TMSI REAL LOCATION COMPLETE 消息来进行确认。

VLR 收到 TMSI 重分配确认后，开始释放信令连接。Iu 接口通过 RANAP IU RELEASE 命令释放，RNC 接收这个命令后释放 RRC 连接。连接释放后，RNC 向 MSC 服务器发送 RANAP IU RELEASE COMPLETE 消息来进行确认。

11.3.4 CN PS 域的路由区更新

如第 6 章所述，CN PS 域自行维护 UE 的位置信息。PS 域虽然也可以识别出 LA，但更有意义的是 RA（Routing Area，路由区）。UE 存储着最后更新过的 RA。UE 从所在小区的系统广播信息中得到当前 RA 的标识。如果它和 USIM 中存储的不同，UE 就启动 RAU（路由区更新）事务，如图 11.21 所示。

UE 先在直接发送消息中发送 GMM RAU REQUEST 消息。该消息包含了旧的和新的 RA 标识。该消息通过 Iu 接口到达新 SGSN。新 SGSN 知道“MM 环境”（即周边的 RA 及与其他 SGSN 的关系）。新 SGSN 根据这个信息得知旧 SGSN，向其发送 GTP-C SGSNCONTEXT REQUEST 消息来得到用户信息。也即新 SGSN 可得知正在进行 RAU 的 UE 是否存在 PDP 报文。

然后，新 SGSN 向用户的 AuC 请求鉴权向量。AuC 计算出后通过 MAP SEND PARAMETERS 消息返回给新 SGSN。现在新 SGSN 就可以为 UE 提供 UTRAN 的鉴权和安全机制。完成鉴权和安全处理后，新 SGSN 发送 GTP－C UPDATE PDP CONTEXT 消息给 GGSN，告诉它 SGSN 已经改变并且 PDP 报文也已相应改变。

此时，新 SGSN 向 HLR 发送 MAP UPDATE LOCATION 消息来更新位置信息，HLR 收到消息后从旧 SGSN 中取消 UE 旧的位置信息，然后发送 MAP INSERT SUBSCRIBER DATA 消息来传送用户配置给新 SGSN。

新 SGSN 更新了用户配置后发送 GMM RAU ACCEPTED 给 UE，该消息包含 UE 的新 P－TMSI。UE 把 P－TMSI 存储在 USIM 中，并发送 GMM ACKNOWLEDGEMENT 消息给 SGSN 以作为接收确认。这样 RA 更新就完成了，新 SGSN 释放此事务所用的信令连接。图 11.21 所示的消息流示出了 SGSN 发生改变时的 RAU。SGSN 并不是在所有 RA 更新中都要改变。SGSN 不变时的过程要简单一些，因为此时不需要 SGSN 和 HLR 之间的 MAP 对话。

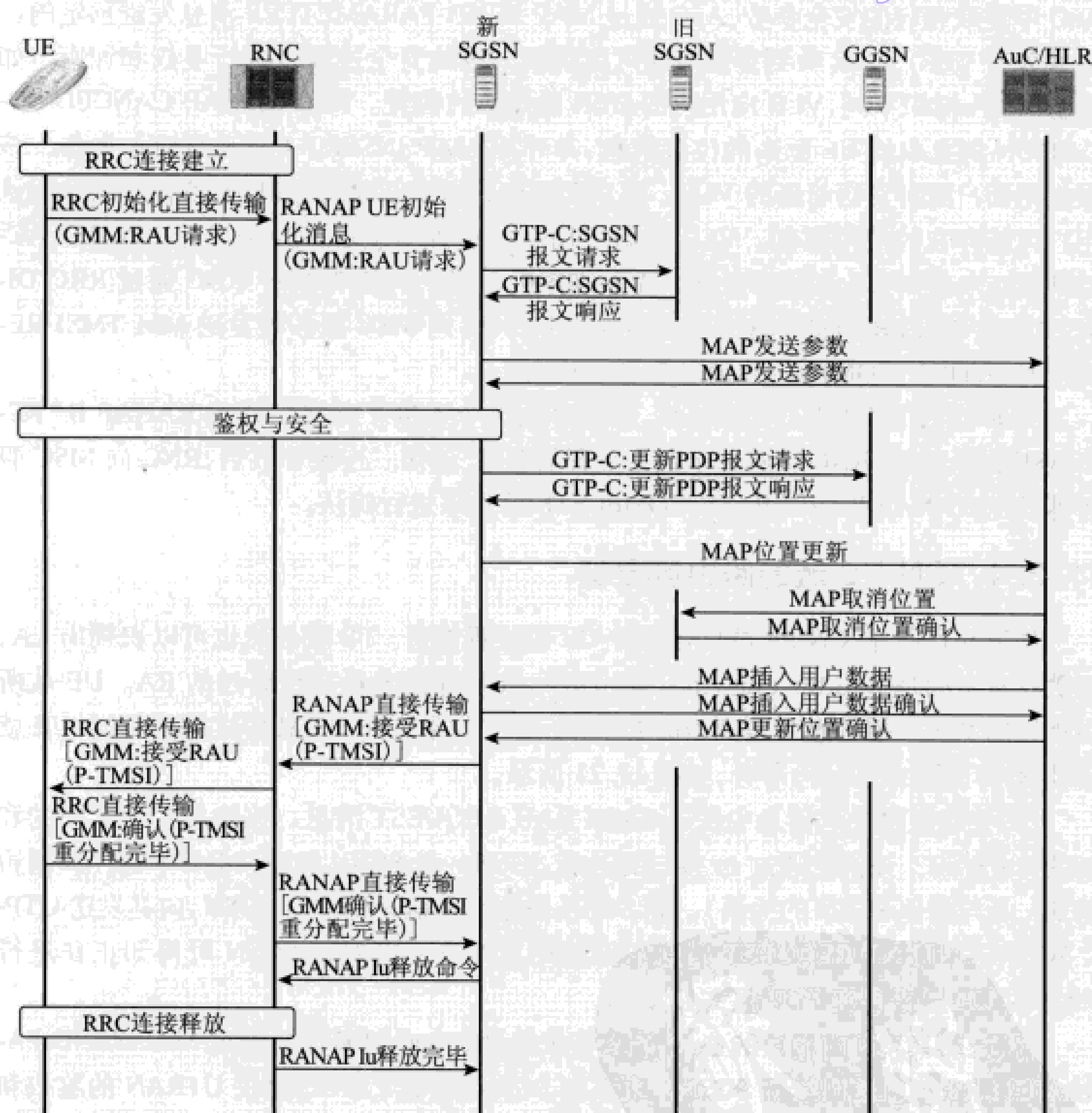


图 11.21　CN PS 域的路由区更新

11.4　CC 过程实例

图 11.22 示出了 PSTN 主叫、UE 被叫的 CS 呼叫的信令消息流，假设 PSTN 信令以及 MSC 节点之间的信令都是 ISUP（ISDN User Part）。

呼叫信令首先通过 ISUP INITIAL ADDRESS MESSAGE（IAM）从 PSTN 进入网关 MSC。该消息包含被叫 UMTS 用户的 MSISDN 号码，这个号码也同时标识了需要使用的业务类型。为了建立 UMTS 网络（CS－MGW）和 PSTN 之间的 CS 通道，GMSC 用 ISUP ADDRESS COMPLETE MESSAGE（ACM）作出响应。

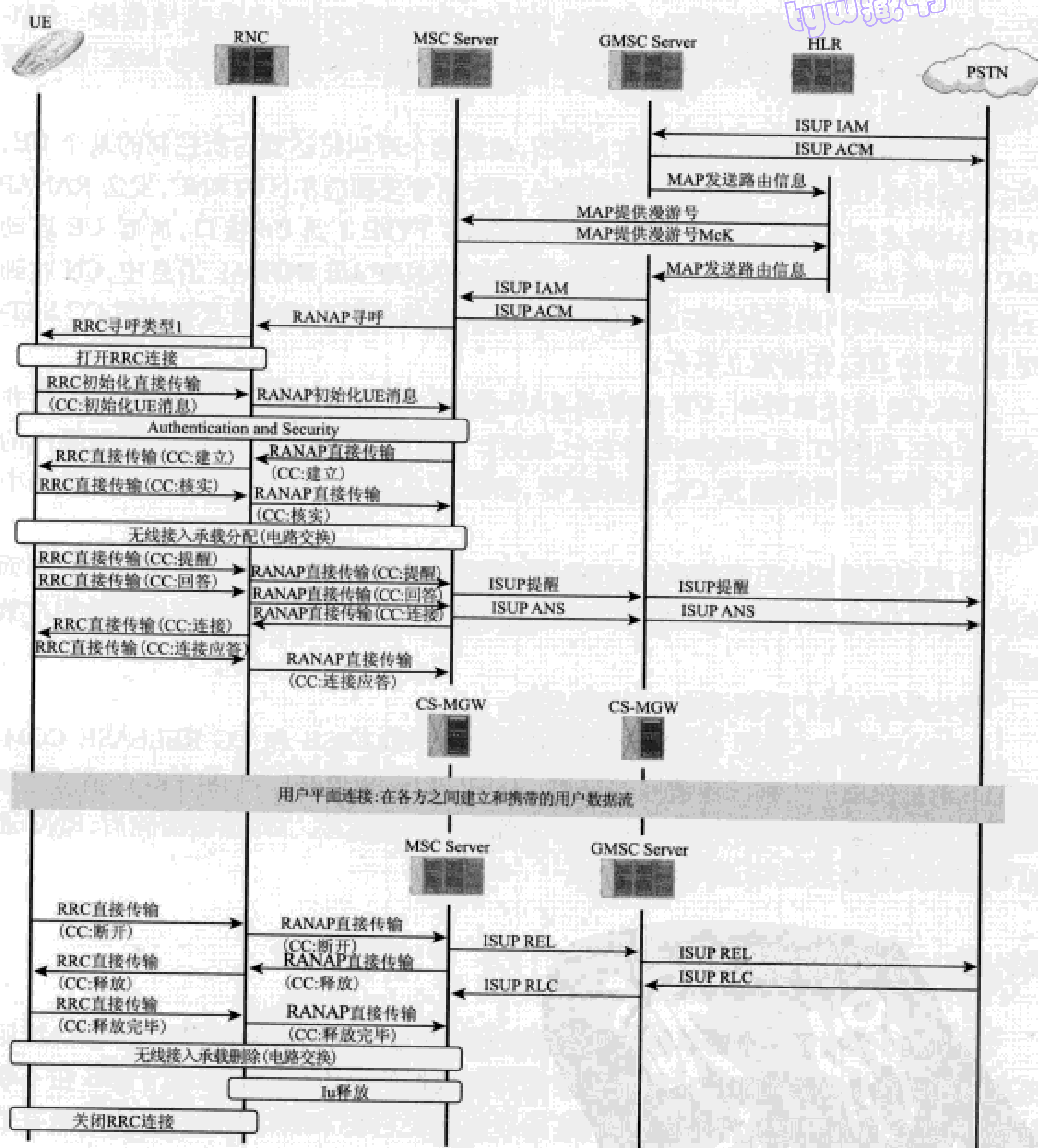


图 11.22　CS 呼叫—UE 被叫—UE 清除

GMSC 发送 MAP SEND ROUTING INFORMATION 消息,请求 HLR 为该用户提供路由信息。GMSC 在这个消息中把接收到的 MSISDN 号码发送给 HLR,HLR 根据这个号码得到用户的 IMSI,同时得到该用户最后一次报告的位置,位置精度是当前 MSC 服务器地址。然后 HLR 向这个 MSC 服务器发送 MAP PROVIDE ROAMING NUMBER REQUEST 消息,服务器为 CS 通道连接分配并返回 MSRN(移动台漫游号),HLR 收到后转发给 GMSC。

MSRN 包含着必要的呼叫路由信息,这是因为网络中的每个 MSC 服务器都

按一定的编号范围分配MSRN,GMSC的CC实体能够识别出其编号范围。GMSC使用接收到的MSRN并通过ISUP IAM和ISUPACM消息实现到MSC服务器的呼叫路由。

MSC服务器识别出它所分配的MSRN,确定这个呼叫将达到它所控制的某个UE,然后根据目标UE最后一次位置更新的LA确定出管理相应小区的RNC,发送RANAP寻呼消息给这些RNC。RNC发送RRC PAGING TYPE I到Uu接口,所呼UE启动RRC连接建立过程。对寻呼的实际响应包含在RANAP UE INITIAL消息中,CN收到后开始进行该呼叫的鉴权和安全工作。然后CN将这个到达呼叫及其特性用CC SETUP消息发给UE,开始建立事务。

如果UE接受该呼叫,CN将启动RAB分配。分配RAB后,UE向用户振铃并且通过CC ALERT消息通知网络它已振铃。这个信息通过网络到达主叫用户的交换机。用户接听将触发CC连接过程,接听信息通过ISUP ANS消息在网络中传输。

CS呼叫通道现在已经能通过MSC和GMSC控制的CS媒体网关。因为用户平面连接已经打开,所以计费开始、相关的语音编码器开始工作、系统可以开始传输用户数据流。

在本实例中我们还假设由UE清除连接。

UTRAN中通过交换CC DISCONNECT、CC RELEASE和CC RELEASE COMPLETE消息使用了一种三步清除的过程。ISUP端用ISUPREL和ISUPRLC消息完成相同的工作。这些消息停止所有计费,并清除节点间的连接。CS通道清除后,RNC通过Iu释放过程释放RAB和RRC连接。

11.5 分组数据实例

图11.23示出了一个简单的分组会话实例。在这里我们也假设UE在UTRAN服务区内连续移动,UE的用户应用希望发送分组数据给网络(上行)。由于UE在不断移动,所以它首先需要执行小区更新,这样才能保证它在SRNC中的位置信息是有效的,位置需要精确到小区。

小区更新后,UE可以通过当前小区请求PDP报文激活,同时可以建立一个用于分组数据传输的RAB。图11.8示出了该过程所涉及的完整消息流。分组会话打开后,UE传输上行数据分组,它先通过形成无线承载的无线链路到达SRNC,然后用GTP-U协议进入RNC和GGSN之间的隧道。隧道在物理上由两部分组成:在Iu接口上的Iu承载、在SGSN和GGSN之间的PS域主干承载。隧道在GGSN结束,此后用户分组数据根据PDP报文中的连接类型参数继续在外部分组数据网络中传输。这个参数的值可能是PPP(点到点协议)或者X.25之类。不再有数据需要传输时,去激活PDP报文,释放RAB。去激活所涉及的完整消息流如图11.11所示。

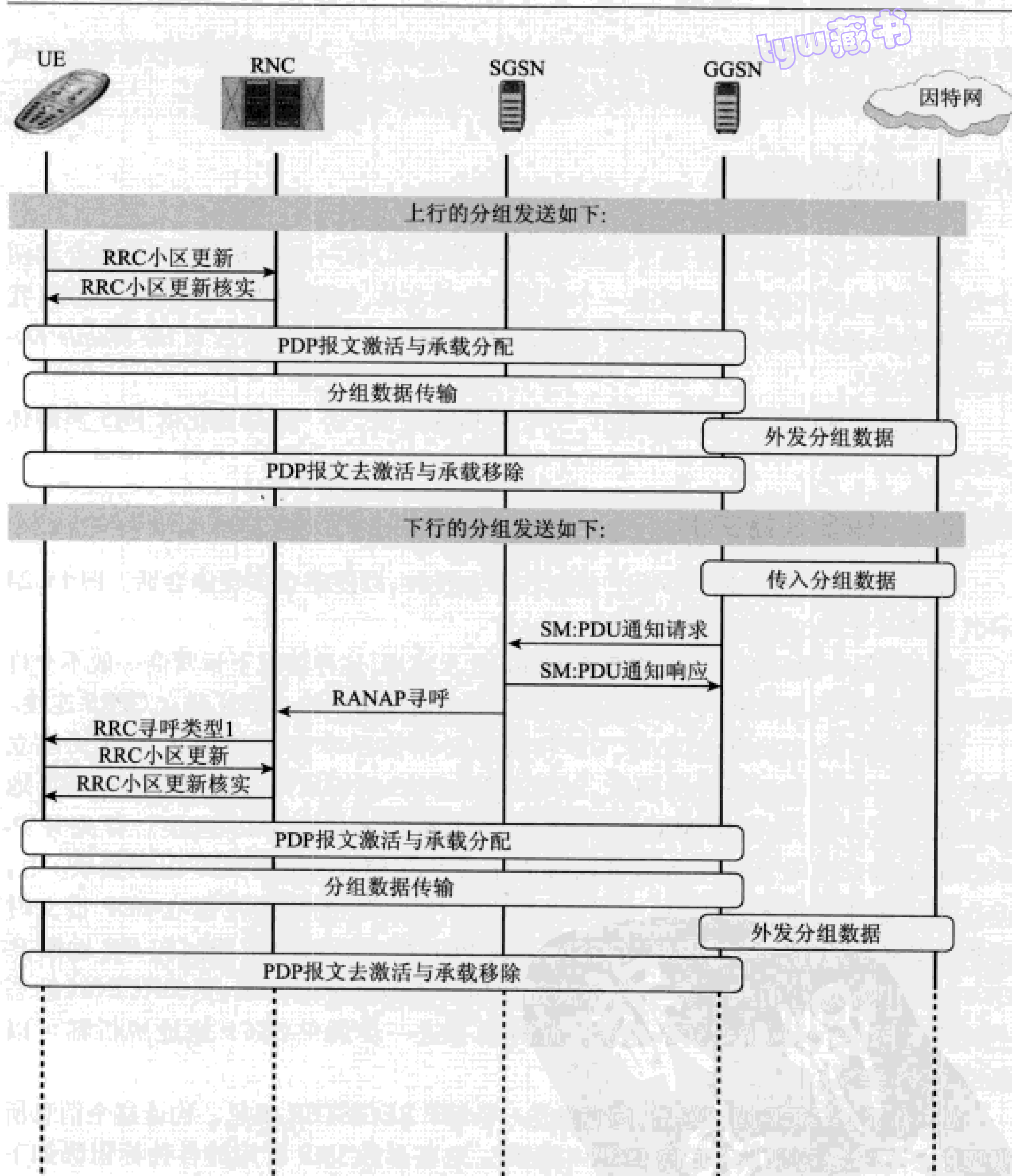


图 11.23　分组数据交换——上行和下行

在下行方向，GGSN 可能要晚一些才知道有分组从其他网络到来。之后触发 SM PDU NITIFICATION 过程，它使网络启动 PDP 报文激活。SGSN 收到 SM PDU NITIFICATION REQUEST 消息后发送到这样一些 RNC，它们控制着 UE 最后一次执行 RA 更新所报告的 RA。RNC 按 RRC PAGING TYPE I 向 UE 发送寻呼。因为 UE 在不断移动，所以它必须再次进行小区更新以使 RNC 记录的小区信息有效。

小区更新后，PDP 报文和 RAB 处于激活状态，并且开始从 GGSN 传输数据分组业

务到 UE。如果此时 UE 有数据需要传输，可以同时进行。上行数据传输按前述的方式处理。当没有数据需要传输时，再次去激活 PDP 报文并释放 RAB。

11.6 IMS 实例

到目前为止我们已经介绍了 IMS 的结构（第 6 章）和一些业务实例。本节介绍两个 IMS 功能的简化实例。IMS 是一个相对复杂的实体，如希望进一步理解其细节，我们推荐 Poikselka 等所著的 *IMS—IP Multimedia Concepts and Services in the Mobile Domail*（2004 年）。

在我们所选的两个处理过程中，一个是 IMS 注册，另一个是简化的 IMS 多媒体会话。

11.6.1 IMS 注册实例

IMS 注册的目的是对 IMS 用户进行注册和授权，以便建立多媒体会话。图 11.24 示出了 IMS 注册过程的主要内容。

在本实例中我们假定 IMS 在现有 GPRS 之上实现，这种情况下运营商一般不允许使用“万能卡接入点名称”，也就是说，用户必须通过网络中的 GGSN 建立 GPRS 连接。

在建立信令 PDP 报文之前，UE 和网络必须按照本章先前所述的方式建立 RRC 连接。根据前面所说的假设，SGSN 借助 DNS 解析用户归属网络的 GGSN 地址。如果允许用户使用 IMS 业务，需要一些参数来建立 IMS 连接。首先是 P-CSCF（代理 CSCF）地址。虽然可以事先定义并存储在 ISIM（IMS 识别模块）中，但这会让地址空间十分受限。更好的方法是利用 UE 的功能在建立 PDP 报文时请求 P-CSCF 地址。当请求时，GGSN 会在 PDP 报文激活请求期间向 UE 返回 P-CSCF 的 IPv6 地址前缀。另一种办法是使用动态地址分配方案，由 DHCPv6（动态主机配置协议）返回 P-CSCF 地址。此时所有进一步的 P-CSCF 地址解析都可以借助 DNS 完成。

UE 有了 P-CSCF 的地址后，向它发送一条 SIP REGISTER 消息。构造这个消息所需要的一些参数可以从 UE 的 ISIM 中获得。这些参数 IMS 所用的各种标识码如下所示。

- 用户个人标识码。
- 用户公共标识码。因为用户可能有多个这样的标识码，因此 IMS 注册通常将列表上的第一个作为默认标识码。
- 归属网络域。
- 拜访网络分配给 UE 的 IP 地址。

公共及个人标识码的介绍见 6.2.1.1.7 节和 6.2.1.1.8 节，我们将在安全相关的内容中再对个人标识码做简单的讨论。

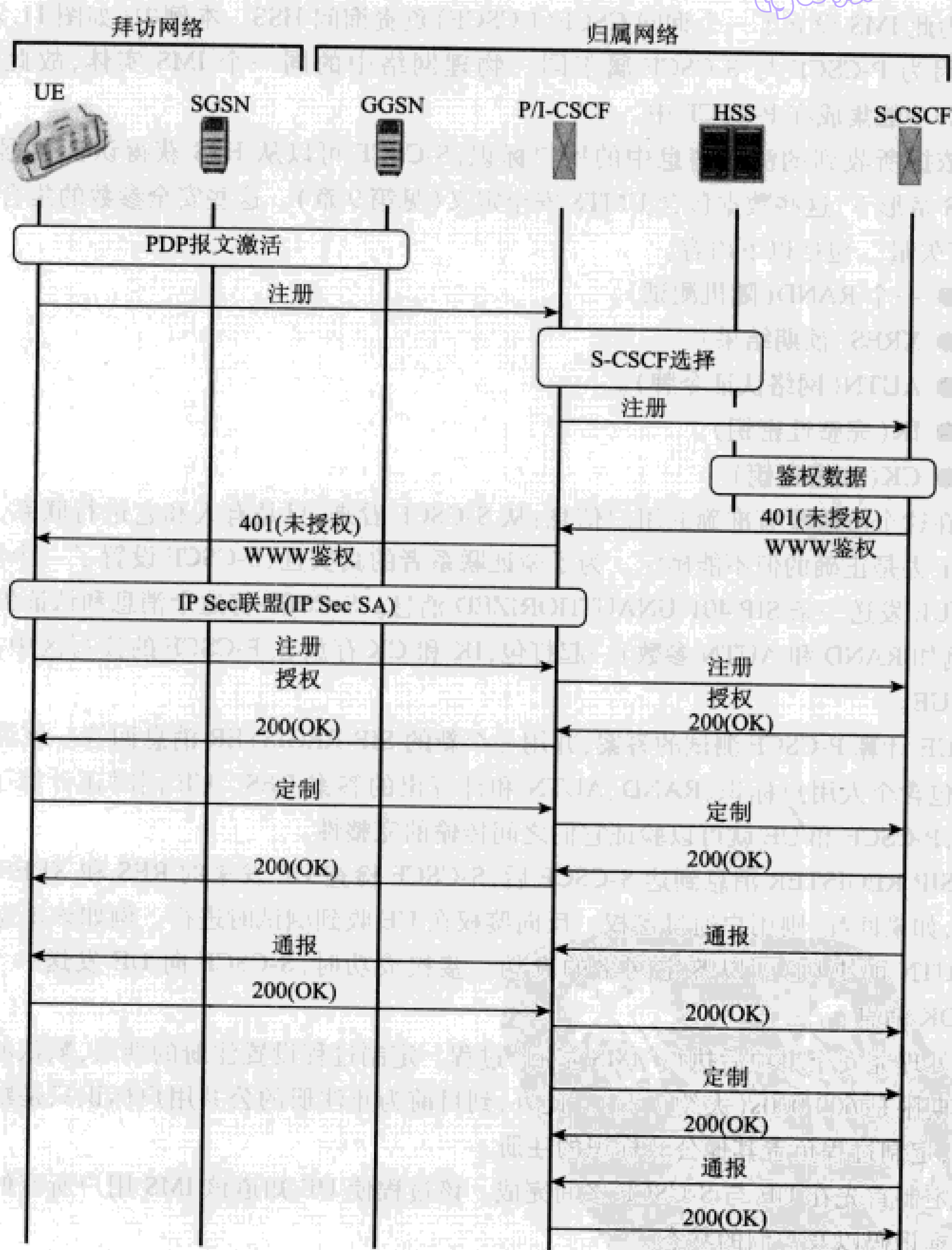


图 11.24 IMS 注册过程

从安全因素考虑，对 IMS 环境最理想的情况是使用 IMS 特定标识。但 UE 并不总存在 ISIM。在这种情况下，就需要通过标准 USIM 来导出标识。为了安全，这个结果不能泄漏到 IMS 环境以外。例如，如果个人用户标识是这样构造的，它将与 IMSI 十分相似。

在 P－CSCF 能够发送注册信息之前，它必须先找到能到达正确的 S-CSCF 的路

由。为此IMS设立了一个询问CSCF(I-CSCF)负责询问HSS。本例中(如图11.24所示),因为P-CSCF与S-CSCF属于同一物理网络中的同一个IMS实体,故此假定I-CSCF功能集成在P-CSCF中。

依据所收到的注册消息中的用户标识,S-CSCF可以从HSS获得认证数据。在UMTS情形下,这些数据包含UMTS安全定义(见第9章)。这些安全参数的集合称为"认证矢量",包括以下内容。

- 一个RAND(随机测试)。
- XRES(预期结果)。
- AUTN(网络认证令牌)。
- IK(完整性密钥)。
- CK(加密密钥)。

在这个阶段没有准确的用户信息:从S-CSCF看来,只是有人和它进行联系,其地址看上去是正确的但不能确定。为了验证联系者的真实性,S-CSCF设置了一个测试。它向UE发送一条SIP 401 UNAUTHORIZED消息。S-CSCF将这个消息和认证矢量数据(例如RAND和AUTN参数)一起打包,IK和CK存放在P-CSCF的读写区中,不会到达UE。

UE计算P-CSCF测试的答案,并用一个新的SIP REGISTER消息回答。该消息这一次包含个人用户标识、RAND、AUTN和计算出的答案RES。UE同时还计算了IK。此时,P-CSCF和UE就可以验证它们之间传输的完整性。

SIP REGISTER消息到达S-CSCF后,S-CSCF检查UE发来的RES和XRES是否匹配,如果匹配,则用户通过鉴权。反向鉴权在UE收到测试时进行。例如该消息包含的AUTN可使UE可以鉴定网络的真伪。鉴权成功时,S-CSCF向UE发送一个SIP 200 OK消息。

处理完安全事项后执行"IMS定制"过程。定制过程设置注册的期限,默认的IMS注册期限是600 000s(大约7天)。此外,到目前为止注册的公共用户标识只是默认的标识,定制过程负责其他公共标识的注册。

定制首先在UE与S-CSCF之间完成。该过程使UE知道该IMS用户所有的公共用户标识码以及它们的状态。

P-CSCF中也必须有相同的信息,因此定制也在P-CSCF和S-CSCF之间单独执行。定制完成后,UE已经与IMS建立连接,可建立多媒体呼叫或使用其他IMS业务。

11.6.2 IMS会话实例

在该实例中,我们说明如何建立IMS会话(如图11.25所示),哪些网元参与用户平面的通信(如图11.26所示),如何清除IMS会话(如图11.27所示)。

拜访网络　归属网络

UE A　P/I-CSCF　S-CSCF　P/I-CSCF　UE B

INVITE　INVITE　INVITE　INVITE

100(尝试)　100(尝试)　100(尝试)

183(会话进行)　183(会话进行)　183(会话进行)　183(会话进行)

PRACK　PRACK　PRACK　PRACK

资源保留

200(OK)　200(OK)　200(OK)　200(OK)

资源保留

UPDATE　UPDATE　UPDATE　UPDATE

200(OK)　200(OK)　200(OK)　200(OK)

180(振铃)　180(振铃)　180(振铃)　180(振铃)

PRACK　PRACK　PRACK　PRACK

200(OK)　B获得

200(OK)　200(OK)　200(OK)

ACK　ACK　ACK　ACK

图 11.25　建立 IMS 会话



图 11.26　IMS 会话的用户平面

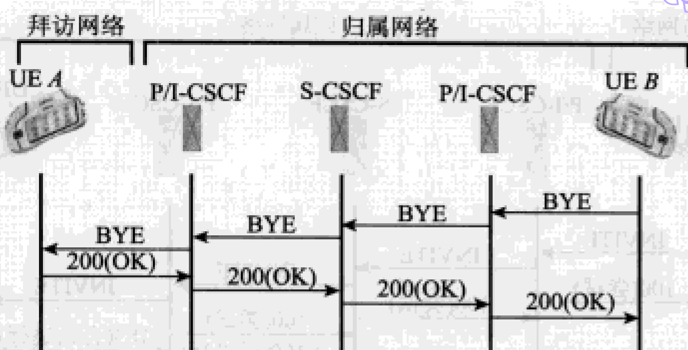


图 11.27　IMS 会话的清除

我们仍然采用和前例相同的假设,即 UE *A* 处于移动状态,GPRS 连接终止于归属网络的 GGSN。UE *B* 位于归属网络中,它和 UE *A* 归属网络相同,并且都进行了 IMS 注册,因此它们能互相通信。

图 11.25 示出了 UE *A* 联系 UE *B* 时的信令图。建立 IMS 会话从 SIP INVITE 请求开始。该请求的头包含两个公共标识:一个用于主叫方(本例的 *A*),一个用于被叫方(本例的 *B*)。P-CSCF 收到这个请求,然后转发到 UE *A* 的 S-CSCF。在此阶段,系统只知道 SIP INVITE 请求的最终目的地(即 UE *B* 注册的公共标识码)。ICSCF 功能联系 HSS,找出该公共标识码的注册地(即哪个 S-CSCF)。之后将 INVITE 请求转给 UE *B* 的 S-CSCF,随后又通过 UE *B* 的 P-CSCF 转发到 UE *B*。为了建立多媒体会话,该 INVITE 请求中包含所有需要的媒体和编码信息,即"第一 SDP 提议"(SDP = 会话描述协议)。

在这个过程中,不同的 CSCF 都会将它们的地址信息附加到 INVITE 请求中。当 INVITE 请求到达 UE *B* 时,UE *B* 又将它自己的 IP 地址添加到列表中,用以说明所涉及的其他所有网元,例如该会话中所有其他消息的地址。UE *B* 还会添加上它为这个会话分配的端口号。这样,随后的所有消息都会使用已经建立的 IPSec SA(IP 安全联盟)。

UE *A* 发送 INVITE 请求时同时启动了一个定时值为 2s 的定时器。在这段时间中,它等待网络的响应,预期的响应是 SIP 183 SESSION PROGRESS。很有可能在预定的 2s 时间内没有响应,因此要用到中间应答 SIP 100 TRYING。SIP 100 TRYING 消息指示 UE *A* 不要重传 INVITE 请求,因为 P-CSCF 将负责所有必要的重传。

SIP 183 SESSION PROGRESS 信息会返回到 UE *A*。UE *A* 的 P-CSCF 是在该消息到达 UE *A* 前最后一个处理它的地方。此时 P-CSCF 将其端口号添加到该消息中,这样在连接中就可以使用 IPSec SA。SIP 183 SESSION PROGRESS 到达 UE *A* 后,它把 UE *B* 的 IP 地址以及出现在消息中的路由信息存储起来。这个消息中包含对原 INVITE 请求中的第一 SDP 提议的响应,该响应包含有关可支持的媒体和编码方面的信息,称其为"第一 SDP 回复"。

收到 SIP 183 SESSION PROGRESS 消息后，UE *A* 用 PRACK 消息应答，也被称为"第二个 SDP 提议"，其中的信息对每个已接受的媒体定义一个编解码。UE *B* 用 SIP 200 OK 对 PRACK 做出应答，表明双方现在已经在所用的编解码和媒体类型方面达成一致，这个应答相应地也称为"第二 SDP 回复"

当双方都已经知道并同意所用的编解码和媒体类型后，开始启动资源预留。资源预留实际上和建立媒体 PDP 报文类似，只是一组用来描述该多媒体会话的用户平面的参数（例如，QoS 定义）。

到目前为止，UE *B* 还没有告知其用户一个到达的多媒体会话即将建立。这是应该的，因为现在还无法保证会话。只有当双方都成功执行了资源预留后才能保证。UE *A* 做完后向 UE *B* 发送 SIP UPDATE 消息，称为"第三个 SDP 提议"，表明资源预留是否成功，所有要求是否满足。如果资源预留也是成功的，UE *B* 就应答以消息 SIP 200 OK，也称为"第三 SDP 回复"。交换该消息后，用户平面的路由就已经完全就绪。

UE *B* 通过 SIP 180 RING 消息告诉 UE *A*，它将向其用户通知到达的多媒体会话。UE *A* 发送 SIP PRACK 消息确认连接状态。UE *B* 的用户摘机后，UE *B* 发送 SIP 200 OK 消息指示用户平面可以打开，其确认应答是 SIPACK。IMS 会话现在已经建立，UE *A* 和 UE *B* 之间可以依照所需并达成一致的媒体类型和编解码进行多媒体连接。图 11.26 示出了用户平面如何经过不同设备的例子。

这个实例假定 UE *B* 清除连接。连接清除从发送 SIP BYE 消息开始。在发送 SIP BYE 消息的同时，UE *B* 退出媒体 PDP 报文，使用户平面关闭。SIP BYE 到达 UE *A* 时，它也会相应退出媒体 PDP 报文。UE *A* 发送 SIP 200 OK 消息作为对 SIP BYE 的应答。这将使所连接的 CSCF 清除所有与此次多媒体会话有关的信息和地址表。

缩略语对照表

16QAM(Quadrature Amplitude Modulation)	十六进制正交幅度调制
3GPP(Third Generation Partnership Project)	第三代移动通信伙伴计划
3GPP2(Third Generation Partnership Project No. 2)	第三代移动通信伙伴计划(2)
8-PSK(Octagonal Phase Shift Keying)	八进制相移键控
AAA(Authentication, Authorisation and Accounting)	鉴权、认证和计费
AAL(ATM Adaptation Layer)	ATM 适配层
ABR(Available Bit Rate)	可用比特速率
AC(Admission Control)	接纳控制
ACM(Address Complete Message)	地址完全消息
ACTS(Advanced Communications Technology and Services)	先进通信技术和服务
ACTS FRAMES(ACTS Future Radio Wideband Multiple Access System)	ACTS 未来无线宽带多址系统
AGCH(Access Grant CHannel)	接入许可信道
AH(Authentication Header)	鉴权头
AICH(Acquisition Indication CHannel)	捕获指示信道
AK(An anonymity key)	匿名密钥
AKA(Authentication and Key Agreement)	鉴权和密钥协商
AM(Acknowledged Mode)	确认模式
AM-SAP(Acknowledged Mode SAP)	确认模式 SAP
AMC(Adaptive Modulation and Coding)	自适应调制编码
AMF(Authentication Management Field)	鉴权管理域
AMPS(American Mobile Phone System)	美国移动电话系统
AMR(Adaptive Multi Rate)	自适应多速率
AOA(Angle Of Arrival)	到达角
AP(Access Point; Application Part)	接入点;应用部分
API(Application Programming Interface)	应用编程接口
APN(Access Point Name)	接入点名
ARIB(Association of Radio Industries and Business)	电波产业协会
AS(Application Server)	应用服务器

ATD(Absolute Time Difference)	绝对时间差
ATM(Asynchronous Transfer Mode)	异步传输模式
AuC(Authentication Centre)	鉴权中心
AUTN(An authentication token)	鉴权令牌
AUTS(An authentication key in re-synchronisation)	在同步中鉴权密钥
AV(Authentication Vector)	鉴权向量
BC(BroadCast)	广播
BCCH(Broadcast Control CHannel)	广播控制信道
BCFE(Broadcast Control Function Entity)	广播控制功能实体
BCH(Broadcast CHannel)	广播信道
BER(Bit Error Rate)	误比特速率
BGCF(Breakout Gateway Control Function)	出口网关控制功能
BICC(Bearer Independent Call Control)	与承载无关的呼叫控制
BMC(Broadcast/Multicast Control)	广播/多播控制
BML(Business Management Layer)	业务管理层
BMP(BitMap Picture)	位图
BS(Base Station (or Node B))	基站
BSC(Base Station Controller)	基站控制器
BSS(Base Station Subsystem;Basic Service Set)	基站子系统;基本业务集
BSSI(Base Station Subsystem Identifier)	基站子系统识别
BSSMAP(Base Station Subsystem MAP)	基站子系统 MAP
BTS(Base Station Transceiver Station)	基站收发信台
CA(Certification Authority)	身份认证
CA-ICH(CPCH Assignment Indication CHannel)	CPCH 分配指示信道
CAMEL(Customised Application for Moblie Network Enhanced Logic)	移动网络定制应用增强逻辑
CAP(CAMEL Application Part)	CAMEL 应用部分
CAPEX(CAPital EXpenditure)	资本开支
CBR(Constant Bit Rate)	恒定比特速率
CC(Country Code;Call Control)	国家代码;呼叫控制
CCA(Clear Channel Assignment)	清除信道指配
CCCH(Common Control CHannel)	公共控制信道
CCF(Charging Collection Function)	计费采集功能
CCH(Communication CHannel)	通信信道
CCK(Complementary Code Keying)	互补码键控
CCPCH(Common Control Physical CHannel)	公共控制物理信道
CD-ICH(Collision Detection Indicator CHannel)	碰撞检测指示信道
CDMA(Code Division Multiple Access)	码分多址

CDR(Charging Data Record) 计费数据记录
CF(Connection Frame) 连接帧
CFN(Connection Frame Number) 连接帧号
CFP(Connection Free Period) 非竞争周期
CGF(Charging Gateway Function) 计费网关功能
CGI(Cell Global Identity) 全球小区识别码
CGW(Charging GateWay) 计费网关
CI(Cell Identity) 小区识别码
CK(Ciphering Key) 密钥
CLP(Cell Loss Priority) 信元丢失优先级
CLPC(Closed Loop Power Control) 闭环功率控制
CM(Code Management;Communication Management;Configuration Management) 码元管理;通信管理;配置管理
CN(Core Network) 核心网
COMC(COMmunication Control) 通信控制
COPS(Common Open Policy Service) 公共开放策略服务
COUNT(A frame-dependent input to A5/3) 与帧号相关的 A5/3 输入
COUNT-C(A frame-dependent input to f8) 与帧号相关的 f8 输入
COUNT-I(A frame-dependent input to f9) 与帧号相关的 f9 输入
CP(Contention Period) 竞争周期
CPC(Centralised Power Control) 集中功率控制
CPCH(Common Packet CHannel) 公共分组信道
CPICH(Common PIlot CHannel) 公共导频信道
CPM(Continuous Power Mode) 连续功率模式
CQI(Channel Quality Indication) 信道质量指示
CRC(Cyclic Redundancy Check) 循环冗余校验
CRNC(Controlling RNC) 控制 RNC
C-RNTI(Cell RNTI) 小区 RNTI
CS(Circuit Switched;Coding Scheme;Convergence Sublayer) 电路交换;编码方法;收敛子层
CS-MGW(Circuit Switched Media GateWay) 电路交换媒体网关
CSCF(Call Session Control Function) 呼叫会话控制功能
CSE(CAMEL Service Environment) CAMEL 服务环境
CSICH(CPCH Status Indicator CHannel) CPCH 状态指示信道
CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance) 碰撞避免的载波监听多址
CSPDN(Circuit Switched Public Data Network) 电路交换公共数据网
CTCH(Common Traffic CHannel) 公共业务信道

CTS(Client To Server)	清除发送
CW(Call Waiting;Carrier Wave;Continuous Wave)	呼叫等待;载波;连续波
CWTS(China Wireless Telecommunication Standard Group)	中国无线通信标准组织
DBPSK(Differential Binary Phase Shift Key)	差分二进制相移键控
DCCH(Dedicated Control CHannel)	专用控制信道
DCF(Distributed Coordination Function)	分布协调功能
DCFE(Dedicated Control Function Entity)	专用控制功能实体
DCH(Dedicated CHannel)	专用信道
DCH-FP(DCH Frame Protocol)	DCH 帧协议
DES(Data Encryption Standard)	数据加密标准
DGPS(Differential GPS)	差分 GPS
DHCP(Dynamic Host Configuration Protocol)	动态主机配置协议
DiffServ(Differentiated Services)	区分服务
DIFS(DCF InterFrame Space)	DCF 帧间间隔
DL(DownLink)	下行
DNS(Domain Name Server)	域名服务器
DoS(Denial of Service)	拒绝服务
DPCCH(Dedicated Physical Communication CHannel)	专用物理公共信道
DPCH(Dedicated Physical CHannel)	专用物理信道
DPDCH(Dedicated Physical Data CHannel)	专用物理数据信道
D-RNTI(Drift RNC Radio Network Temporary Identity)	漂移 RNC 无线网络临时识别码
DQPSK(Differential QPSK)	差分 QPSK
DRNC(Drifting RNC)	漂移 RNC
DRX(Discontinuous Reception)	非连续接收
DS-CDMA(Direct Sequence CDMA)	直接序列 CDMA
DSCH(Downlink Shared CHannel)	下行链路共享信道
DSCH-RNTI(DSCH Radio Network Temporary Identity)	DSCH 无线网络临时识别码
DSCP(Differentiated Services Code Point)	差分服务代码点
DSL(Digital Subscriber Line)	数字用户线
DSSS(Direct Sequence Spread Spectrum)	直接序列扩频
DS-WCDMA-FDD(DS Wideband CDMA Frequency Division Duplex)	DS 宽带 CDMA 频分双工
DS-WCDMA-TDD(DS Wideband CDMA Time Division Duplex)	DS 宽带 CDMA 时分双工
DTCH(Dedicated Traffic CHannel)	专用业务信道
DTX(Discontinuous Transmission)	非连续传输
E-GPRS(Enhanced GPRS)	增强 GPRS

E-OTD(Enhanced Observed Time Difference)	增强型观察时间差
E1(E1 system;European Digital Signal 1)	E1 系统;欧洲数字信号 1
E2E,e2e(End-to-End)	端到端
ECT(Explicit Call Transfer)	明确呼叫转移
EDGE(Enhanced Data for GSM Evolution)	增强数据 GSM 演进
EIR(Equipment Identity Register)	设备识别寄存器
EMC(ElectroMagnetic Compatibility)	电磁兼容
EML(Element Management Layer)	单元管理层
ESP(Encapsulation Security Payload)	封装安全载荷
ETSI(European TelecommunicationS Institute)	欧洲电信标准组织
FACCH(Fast Association Control CHannel)	快速随路控制信道
FACH(Forward Access CHannel)	前向接入信道
FBI(FeedBack Information)	反馈信息
FCH(Frequency correction CHannel)	频率校正信道
FDD(Frequency Division Duplex)	频分双工
FDMA(Frequency Division Multiple Access)	频分多址
FER(Frame Error Rate)	误帧率
FH-CDMA(Frequency Hopping CDMA)	跳频 CDMA
FHSS(Frequency Hopping Spread Spectrum)	跳频扩频
FM(Fault Management)	故障管理
FPS(Fast Packet Scheduling)	快速分组调度
FPLMTS(Future Public Land Mobile Telephony System)	未来公共地面移动电话系统
FR(Frequency Reuse)	频率复用
FRAMES(ACTS Future Radio Wideband Multiple Access System)	ACTS 未来宽带多址系统
FRESH(A one-time random number chosen by the RNC)	RNC 选择的随机码
FW(FireWall)	防火墙
GERAN(GSM/EDGE Radio Access Network)	GSM/EDGE 无线接入网
GGSN(Gateway GPRS Support Node)	网关 GPRS 支持节点
GIF(Graphic Interchange Format (image file))	图形交换格式(图像文件)
GMLC(Gateway Mobile Location Centre)	网关移动位置中心
GMM(GPRS Mobility Management)	GPRS 移动管理
GMSC(Gateway MSC)	网关 MSC
GMSK(Gaussian Minimum Shift Keying)	高斯最小移频键控
GPRS(General Packet Radio Service)	通用分组无线业务
GPS(Global Positioning System)	全球定位系统
GRX(GPRS Roaming Exchange)	GPRS 漫游交换
GSM(Global System for Mobile communication)	移动通信全球系统

GSMS(GPRS SMS)	GPRS SMS
GT(Global Title)	全球标识码
GTD(Geometric Time Difference)	几何时间差
GTP(GPRS Tunnelling Protocol)	GPRS 隧道协议
HARQ(Hybrid Automatic Repeat reQuest)	混合自动重传请求
HCS(Hierarchical Cell Structure)	小区分层结构
HDLC(High-level Data Link Control)	高级数据链路控制
HEC(Header Error Control)	信头差错控制
HFN(HyperFrame Number)	超帧号
HLR(Home Location Register)	归属位置寄存器
HM-CDMA(Hybrid Modulation CDMA)	混合调制 CDMA
HO(HandOver)	切换
HON(HandOver Number)	切换号
HS-DPCCH(High Speed DPCCH)	高速 DPCCH
HS-DSCH(High Speed DSCH)	高速 DSCH
HS-DSCH-FP(High Speed DSCH Frame Protocol)	高速 DSCH 帧协议
HS-PDSCH(High Speed PDSCH)	高速 DSCH
HS-SCCH(High Speed SCCH)	高速 SCCH
HSCSD(High Speed Circuit Switched Data)	高速电路交换数据
HSDPA(High Speed Downlink Packet Access)	高速下行分组接入
HSS(Home Subscriber Server)	归属用户服务器
HSUPA(High Speed Uplink Packet Access)	高速上行分组接入
HTML(HyperText Markup Language)	超文本标记语言
HTTP(HyperText Transfer Protocol)	超文本传输协议
HW(HardWare)	硬件
I-CSCF(Interrogating CSCF)	查询呼叫控制功能
I/O(Input/Output)	输入/输出
IA(Interception Area)	截获区
IAM(Initial Address Message)	初始地址消息
IBSS(Independent Basic Service Set)	独立基本服务集
ICC(Integrated Circuit Card)	集成电路卡
IEEE(Institute of Electrical and Electronic Engineers)	电气电子工程师学会
IETF(Internet Engineering Task Force)	因特网工程任务组
IFS(InterFrame Space)	帧间间隔
IK(Integrity Key)	完整性密钥
IKE(Internet Key Exchange)	因特网密钥交换
IM(IP Multimedia)	IP 多媒体
IMA(Inverse Multiplexing for ATM)	ATM 反向复接

IMEI(International Mobile Equipment Identity)	国际移动设备识别码
IMEISV(IMEI and Software Version)	IMEI 和软件版本号
IMPI(IP Multimedia Private Identity)	IP 多媒体私有用户标识
IMPU(IP Multimedia Public User identity)	IP 多媒体公共用户标识
IMS(IP Multimedia System)	IP 多媒体系统
IMS-MGW(IMS Media GateWay)	IMS 媒体网关
IMS-SF(IMS Switching Function)	IMS 交换功能
IMSI(International Mobile Subscriber Identity)	国际移动用户识别码
IMT(International Mobile Telephony)	国际移动电话
IN(Intelligent Network)	智能网
IP(Internet Protocol)	因特网协议
IPDL(Idle Period DownLink)	闲置期下行链路
IPSec(IP Security)	IP 安全
IPSP(IP Signalling Point)	IP 信令点
IRC(Internet Relay Chat)	因特网中继聊天
ISCP(Interference Signal Code Power)	干扰信号码功率
ISDN(Integrated Services Digital Network)	综合业务数字网
ISHO(InterSystem HandOver)	系统间切换
ISIM(IMS Identity Module)	IMS 识别模块
ISM (Industrial,Scientific and Medical)	工业、科学和医疗
ISO (International Organization for Standardization)	国际标准化组织
ISUP(ISDN User Part)	ISDN 用户部分
ITU(International Telecommunication Union)	国际电信联盟
JPEG(Joint Photographic Experts Group(format for image compression))	联合图像专家组(用于图像压缩格式)
KASUMI(An encryption operation)	一种加密操作
LA(Location Area)	位置区
LAC(Location Area Code)	位置区号
LAI(Location Area Identity)	位置区识别码
LAN(Local Area Network)	局域网
LCS(LoCation Service)	定位服务
LDP(Label Distribution Protocol)	标记分发协议
LIF-MLP(LIF Mobile Location Protocol)	LIF 移动位置服务协议
LMU(Location Measurement Unit)	位置测量单元
LOS(Line Of Sight)	视距
LSP(Label Switched Path)	标签交换路由
LSR(Label Switching Router)	标签交互路由器
M3UA(MTP3 User Adaptation)	MTP3 用户适配

MAC(Medium Access Control;Message Authentication Code)	媒体接入控制;消息鉴权码
MAC-I(A message authentication code for integrity protection)	用于完整性保护的消息鉴权码
MAC-S(A message authentication code for re-synchronisation)	用于重同步的消息鉴权码
MAP(Mobile Application Part)	移动应用部分
MAPSec(MAP Security)	MAP 安全
MC-CDMA(MultiCarrier CDMA)	多载波 CDMA
MCC(Mobile Country Code)	移动国家码
MCS(Modulation Coding Scheme)	调制编码方案
ME(Mobile Equipment)	移动设备
MEHO(Mobile Evaluated HandOver)	移动台发起的切换
MGCF(Media Gateway Control Function)	媒体网关控制功能
MGCP(Media Gateway Control Protocol)	媒体网关控制协议
MGW(Media GateWay)	媒体网关
MIB(Master Information Block)	主信息块
MM(Mobility Management)	移动性管理
MMS(Multimedia Messaging Service)	多媒体消息业务
MNC(Mobile Network Code)	移动网络码
MO(Mobile Originated (Originating))	移动台主叫
MOBC(MOBility Control)	移动性控制
MOC(Mobile Originated (Originating) Call)	移动台主叫
MPDU(MAC Protocol Data Unit)	MAC 协议数据单元
MPLS(Multi Protocol Label Switching)	多协议标签交换
MRC(Maximum Ratio Combining)	最大比合并
MRFC(Multimedia Resource Function Controller)	多媒体资源功能控制器
MRFP(Multimedia Resource Function Processor)	多媒体资源功能处理器
MS(Mobile Station)	移动台
MSC(Mobile service Switching Centre)	移动业务交换中心
MSIN(Mobile Subscriber Identification Number)	移动用户识别码
MSISDN(Mobile Subscriber ISDN)	移动用户 ISDN
MSN(Mobile Subscription Number)	移动用户号码
MSRN(Mobile Station Subscriber Roaming Number)	移动台用户漫游号
MT(Mobile Terminated (Terminating))	移动终端
MTC(Mobile Terminated (Terminating) Call)	移动台被叫
MTP-3B(Message Transfer Part-3B(Broadcast))	宽带消息传输部分第 3 级(广播)
MTP3(Message Transfer Part Layer 3)	消息传输部分第 3 级

MTU(Maximum Transmission Unit)	最大传输单元
N-ISDN(Narrowband ISDN)	窄带 ISDN
NAS(Network Application Server;Non Access Stratum)	网络应用服务;非接入层
NAV(Network Allocation Vector)	网络分配向量
NBAP(Node B Application Protocol)	基站应用协议
NDC(National Destination Code)	国内终端码
NE(Network Element)	网络单元
NEHO(Network Evaluated HandOver)	网络发起的切换
NEL(Network Element Layer)	网元层
NLOS(Non Line Of Sight)	非视距
NMC(Network Management Centre)	网管中心
NML(Network Management Layer)	网管层
NMS(Network Management Subsystem)	网管子系统
NMT(Nordic Mobile Telephone)	北欧移动电话
NRT(Non Real Time)	非实时
NSS(Network SubSystem)	网络子系统
NT(Network Termination)	网络终端
O&M(Operation and Maintenance)	运维
OCS(Online Charging System)	在线计费系统
OFDMA(Orthogonal Frequency Division Multiple Access)	正交频分多址
OHG(Operator Harmonisation Unit)	运营商协调组织
OLPC(Open Loop Power Control)	开环功率控制
OMA(Open Mobile Alliance)	开放移动联盟
OMC(Operation and Management Centre)	运行与管理中心
OPEX(Operation and Maintenance EXpenditure)	运维费
OSA(Open Service Architecture)	开放业务体系结构
OSA/SCS(OSA/Service Capability Server)	OSA/业务能力服务器
OSI(Open System Interconnection)	开放系统互连
OTD(Observed Time Difierence)	观察时间差
OTDOA(Observed Time Difierence Of Arrival)	观察到达时间差
PA(Paging Area)	寻呼区
PACCH(Packet Access Control CHannel)	分组接入控制信道
PAGCH(Packet Access Grant CHannel)	分组接入许可信道
PAR(Peak Average Rate)	峰均比
PBCC(Packet Binary Convolution Code)	分组二进制卷积码
PBS(Physical Bearer Service)	物理承载业务
PC(Power Control)	功率控制
PCCH(Paging Control CHannel)	寻呼控制信道

P-CCPCH(Primary CCPCH) 主 CCPCH
PCF(Point Coordination Function) 点协调功能
PCH(Paging CHannel) 寻呼信道 PCM;脉冲编码调制
PCPCH(Physical Communication Packet Channel) 物理公共分组信道
PCS(Personal Communication System) 个人通信系统
P-CSCF(Proxy CSCF) 代理 CSCF
PD(Protocol Discriminator) 协议鉴别器
PDC(Pacific Digital Communications) 太平洋数字蜂窝通信
PDCP(Packet Data Convergence Protocol) 分组数据会聚协议
PDF(Policy Decision Function) 决策功能
PDH(Plesiochronous Digital Hierarchy) 准同步数字体系
PDP(Packet Data Protocol) 分组数据协议
PDSCH(Physical Downlink Shared CHannel) 物理下行链路共享信道
PDTCH(Packet Data Traffic CHannel) 分组数据业务信道
PDU(Packet Data Unit;Protocol Data Unit) 分组数据单元;协议数据单元
PGP(Pretty Good Privacy) 良好隐私
PICH(Paging Indicator CHannel) 寻呼指示信道
PIFS(Point coordination function IFS) 点协调功能 IFS
PKI(Public Kev Infrastructure) 公开密钥体系
PLMN(Public Land Mobile Network) 公共陆地移动电话网
PLMN-ID(PLMN Identity) PLMN 标识
PM(Performance Management) 性能管理
PMM(Packet MM) 分组 MM
PN(Pseudo Noise) 伪噪声
PNCE(Paging and Notification Control Entity) 寻呼及布告控制实体
PNG(Portable Network Graphics) 便携网络地图
POC(PSTN Originated(Originating)Call) PSTN 主叫
PoC(Push to talk over Cellular) 蜂窝对讲
PPCH(Packet Paging CHannel) 分组寻呼信道
PPP(Point-to-Point Protocol) 点到点协议
PRACH(Packet Random Access CHannel) 分组随机接入信道
PRACK(Provisional Response ACKnowledgement) 临时响应确认
PRN(Pseudo-Random Numerical) 伪随机序列
PS(Packet Switched;Packet Scheduler) 分组交换;分组调度
P-SCH(Primary SCH) 主 SCH
PSM(Power Save Mode) 节电模式
PSPDN(Packet Switched Public Data Network) 分组交换公共数据网
PSTN(Public Switched Telephone Network) 公共交换电话网

PT(Payload Type)	负荷类型
PTC(PSTN Terminated(Terminating)Call)	PSTN 被叫
P-TMSI(Packet TMSI)	分组 TMSI
QoS(Quality of Service)	服务质量
QPSK(Quadrature Phase Shift Keying)	四相移相键控
RA(Routing Area;Receiver Address)	路由区;接收机地址
RAB(Radio Access Bearer)	无线接入承载
RAC(Routing Area Code)	路由区代码
RACE(Research in Advanced Communications in Europe)	欧洲先进通信技术研究
RACH(Random Access CHannel)	随机接入信道
RADIUS(Remote Authentication Dial In User Service)	用户服务中远程鉴权拨号
RAI(Routing Area Identity)	路由区识别号
RAN(Radio Access Network)	无线接入网络
RANAP(RAN Application Part	RAN 应用部分
RAND(A random(authentication)number)	鉴权中的一种随机挑战
RAP(Random Access Procedure)	随机接入过程
RAU(Routing Area Update)	路由区更新
RES(An authentication response)	鉴权响应
RFC(Request For Comment)	请求注解
RFE(Routing Function Entity)	路由功能实体
RL(Radio Link)	无线链路
RLC(Radio Link Control)	无线链路控制
RLC-SQN(RLC SeQuence Number)	RLC 序列号
RNBP(Reference Node Based Positioning)	基于参考节点的定位
RNC(Radio Network Controller)	无线网络控制器
RNS(Radio Network Subsystem)	无线网络子系统
RNSAP(Radio Network Subsystem Application Part)	无线网络子系统应用部分
RNTI(Radio Network Temporary Identity)	无线网络临时标识
ROHC(RObust Header Compression)	可靠头压缩
RR(Radio Resource)	无线资源
RRC(Radio Resource Control)	无线资源控制
RRM(Radio Resource Management)	无线资源管理
RSVP(ReSerVation Protocol)	资源预留协议
RT(Radio Termination;Real Time)	无线终端;实时
RTD(Relative Time Difference)	相对时间差
RTP(Real Time Protocol)	实时协议
RTS(Request To Send)	请求发送
RTT(Round Trip Time)	往返时间

Rx(Receiving)	接收
S-CCPCH(Secondary Communication Control Physical CHannel)	辅助公共控制物理信道
S-MIME(Secured Multipurpose Internal Mail Extension)	安全的多用途网际邮件扩充协议
S-RNTI(SRNC Radio Network Temporary Identity)	SRNC 无线网络临时识别码
S-SCH(Secondary SCH)	辅助 SCH
SA(Security Association)	安全协会
SAC(Service Area Code)	服务区域代码
SACCH(Slow Associated Control CHannel)	慢速随路控制信道
SAI(Service Area Identity)	服务区识别码
SAP(Service Access Point)	服务接入点
SAR(Segmentation And Re-assembly)	分段与重组
SAW(Stop And Wait)	停等协议
SB(Scheduling Block)	调度块
SBLP(Service Based Local Policy)	基于服务的本地策略
SCCP(Signalling Connection Control Part)	信令连接控制部分
SCH(Synchronisation CHannel)	同步信道
SCCH(Synchronisation Control CHannel)	同步控制信道
SCI(Subscriber Controlled Input)	用户控制输入
SCR(System Chip Rate)	系统码片速率
SCS(Service Capability Server)	业务能力服务器
SCTP(Stream Control Transport Protocol)	流控制传输协议
SDCCH(Stand-alone Dedicated Control CHannel	独立专用控制信道
SDH(Synchronous Digital Hierarchy)	同步数字体系
SDP(Session Description Protocol	会话描述协议
SDU(Signalling Data Unit)	信令数据单元
SEG(SEcurity Gateway)	安全网关
SF(Spreading Factor)	扩频因子
SFN(System Frame Number)	系统帧号
SGSN(Serving GPRS Support Node)	服务 GPRS 支持节点
SGW(Signalling GateWay)	信令网关
SHA-1(Secure Hash Algorithm #1)	安全 Hash 算法 1
SIB(System Information Block)	系统信息块
SIFS(Short IFS)	短 IFS
SIGTRAN(Special Interest Group TRAN)	信令传输特别工作组
SIM(Subscriber Identity Module)	用户识别模块
SIP(Session Initiation Protocol)	会话起始协议
SLA(Service Level Agreement)	服务等级协议

SLF(Subscription Locator Function)	用户定位功能
SML(Service Management Layer)	业务管理层
SMLC(Serving Mobile Location Centre)	服务移动位置中心
SMS(Short Message Service)	短消息业务
SMSC(Short Message Service Centre)	短消息业务中心
SN(Serving Network)	服务网络
SN(Subscriber Number)	用户号
SPC(Signalling Point Code)	信令点代码
SQN(SeQuence Number)	序列号
SRB(Signalling Radio Bearer)	信令无线承载
SRNC(Serving RNC)	服务 RNC
SS(Supplementary Service)	补充业务
SS7(Signalling System #7)	7 号信令系统
SSDT(Site Selective DiversiTy)	站点选择分集
SSL(Secure Socket Layer)	安全套接层
STM(Synchronous Transport Module)	同步传输模式
SVN(Software VersioN)	软件版本
SW(SoftWare)	软件
TA(Timing Advance;Transmitter Address)	定时提前;发射机地址
TAC(Type Allocation Code)	类型分配码
TCAP(Transaction Capabilities Application Part)	事务处理能力应用部分
TCH(Traffic CHannel)	业务信道
TCP(Transmission Control Protocol)	传输控制协议
TDD(Time Division Duplex)	时分双工
TDM(Time Division Multiplexing)	时分复用
TDMA(Time Division Multiple Access)	时分多址
TDOA(Time Difference Of Arrival)	到达时间差
TE(Terminal Eequipment)	终端设备
TEID(Tunnel Endpoint IDentifier)	隧道端点标识
TFCI(Transport Format Combination Indicator)	发送格式组合指示
TFRC(Transport Format and Resource Combination)	发送格式和资源组合
TFRI(Transport Format and Resource Indicator)	发送格式和资源指示
TH-CDMA(Time Hopping CDMA)	跳时 CDMA
THIG(Topology Hiding Inter-network Gateway)	拓扑隐藏网际网关
TI(Standardisation Committee of TI Communications)	TI 通信标准委员会
TI(Transaction Identifier)	事务处理标识
TLS(Transport Layer Security)	传输层安全
TMN(Telecommunications Management Network)	电信管理网络

TM-SAP(Transparent Mode SAP)	透明模式 SAP
TMSI(Temporary Mobile Subscriber Identity)	临时移动台识别码
TOA(Time Of Arrival)	到达时间
TPC(Transmission Power Command;Transmit Power Control)	发送功率指令;发送功率控制
Tr(Transparent mode)	透明模式
TRAU(Transcoding and Rate Adaptation Unit)	编码变换和速率自适应单元
TRX(Transmitter-Receiver)	收发机
TTA(Telecommunications Technology Association)	电信技术协会
TTC(Telecommunications Technology Committee)	电信技术委员会
TTI(Transmission Time Interval)	传输时间间隔
TTP(Traffic Termination Point)	业务终止点
Tx(Transmitting)	发射机
U-RNTI(UTRAN Radio Network Temporary Identity)	UTRAN 无线网络临时标识
UA(User Agent)	用户代理
UBR(Unspecified Bit Rate)	不定比特速率
UDP(User Datagram Protocol)	用户数据包协议
UE(User Equipment)	用户设备
UICC(Universal Integrated Circuit Card)	通用集成电路卡
UL(UpLink)	上行链路
UM(Unacknowledged Mode)	非确认模式
UM-SAP(Unacknowledged Mode SAP)	非确认模式 SAP
UMSC(UMTS Mobile service Switching Centre)	UMTS 移动业务交换中心
UMTS(Universal Mobile Telecommunication System)	通用移动电信系统
UNI(User Network Interface)	用户网络接口
UNII(Unlicensed National Information Infrastructure)	无需许可的国家信息基础设施(频段)
URA(UTRAN Registration Area)	UTRAN 注册区
USAT(UMTS SIM Application Toolkit)	UMTS SIM 应用工具箱
USIM(Universal Subscriber Identity Module)	通用用户识别模块
UTRA(Universal Terrestrial Radio Access)	通用陆地无线接入
UTRAN(UMTS Terrestrial Access Network)	UMTS 陆地无线接入
UWB(Ultra WideBand)	超宽带
VAS(Value Added Service)	增值业务
VBR(Variable Bit Rate)	可变比特速率
VC(Virtual Channel)	虚信道
VCI(Virtual Channel Identifier)	虚信道标识
VLR(Visitor Location Register)	访问位置寄存器
VMS(Voice Mail System)	语音邮件系统

VMSC(Visited MSC)	访问 MSC
VoIP(Voice over IP)	基于 IP 的语音传输
VP(Virtual Path)	虚路径
VPI(Virtual Path Identifier)	虚路径标识
VPN(Virtual Public Network)	虚拟公共网络
VSF(Variable Switching Function)	可变扩频因子
WAP(Wireless Application Protocol)	无线应用协议
WCDMA(Wideband CDMA)	宽带 CDMA
WEP(Wired Equivalent Privacy)	有线等价加密
Wi-Fi(Wireless Fidelity Alliance)	无线保真联盟
WLAN(Wireless LAN)	无线局域网
WML(Wireless Markup Language)	无线标记语言
WRC(World Radiocommunication Conference)	世界无线通信会议
WTLS(Wireless Transport Layer Security)	无线传输层安全
XHTML(Extended HTML)	扩展的 HTML
XMAC(An expected MAC value)	预期 MAC 值
XRES(An expected RES value)	预期 REX

参考文献

对于感兴趣的读者，本参考文献目录包括以下几个方面的技术标准和其他文献。

- 无线通信，尤其是 CDMA 系统。
- 3GPP 技术标准。
- ATM 网络和协议。
- IP 网络和协议。
- 移动定位。
- 安全算法和协议。

对于进一步的阅读来说，这些材料是一个很好的起点。

1. 技术标准

在如今这个时代，公开的技术标准很容易在万维网中查到。下面的 URL 可以连接到对应的网站。

- 3GPP 技术标准：http://www. 3gpp. org。

本书涉及的 3GPP 标准大多来自 R5。可以通过数字格式的参考，如 TS12. 345，来浏览 3GPP 网站上的标准清单。

- IFTF（因特网工程任务组）标准：http://www. ietf. org。

本书中涉及的 IETF 标准都是以 RFC 号给出的（请求注解），可通过 RFC 号在 IETF 网站上查到。

- IEEE 标准：http://standards. ieee. org。

IEEE 系列标准，如 802. 11，可以在 IEEE 网站上找到。

2. 其他文献

Ahonen T and Barrett J(eds)(2002). *Services for UMTS*(373 pp.). Chichester, UK: John Wiley & Sons.

Black U(1998). *ATM*, Vol. Ⅱ: *Signaling in Broadband Networks*(224 pp .). Englewood Cliffs, NJ: Prentice Hal.

Black U(1999). *ATM*, Vol. Ⅰ: *Foundation for Broadband Networks*(450 pp .). Englewood Cliffs, NJ: Prentice Hall.

Comer DE (2000). *Internetworking with TCP/IP*, Vol, I: *Principles, Protocols and Architecture* (4th edn, 755 pp.). Englewood Cliffs, NJ: Prentice Hall.

Doraswamy N and Harkins D(1999). *IPSec:The New Security Standard for the Internet, Intranets, and Virtual Private Networks* (216 pp.). Englewood Cliffs, NJ: Prentice Hall.

Ericsson Telecom AB(1997). *Understanding Telecommunications* (Ⅰ-2, Vol. 1 = 493 pp., Vol. 2 = 677 pp.). Studentlitteratur AB.

Glisic S and Vucetic B(1997). *Spread Spectrum CDMA Systems for Wireless Communications*(383 pp.). Boston: A-H Publishers.

Halonen T, Romero J and Melero J(2002). *GSM. GPRS and EDGE Performance*(585 pp.). Chichester. UK: John Wiley & Sons.

Händel R, Huber MN and Schröder S(1994). *ATM Networks, Corncepts, Protocols, Applications*(2nd edn, 287 pp.). Reading, MA: Addison-Wesley.

Heine G(1998). *GSM Networks: Protocols, Terminology and Implementation* (416 pp.). Boston, MA: Artech House.

Hillebrand F(2002). *GMS and UMTS: The Creation of Global Mobile Communication* (580 pp.). Chichester, UK: John Wiley & Sons.

Holma H and Toskala A (2004). *WCDMA for UMTS*(3rd edn, 450 pp.). Chichester, UK: John Wiley & Sons.

Laiho J, Wacker A and Novosad T(2002). *Radio Network Planning and Optimization for UMTS*(484 pp.). Chichester, UK: John Wiley & Sons.

Kilkki K (2001). *Differentiated Quality of Service for the Internet* (384 pp.). Basingstoke, UK: Macmillan.

Lee WCY(1995). *Mobile Cellular Telecommunications: Analog and Digital Systems* (2nd edn, 664 pp.). New York: McGraw-Hill.

Manterfield R(1999). *Telecommunications Signalling*(435 pp.). The Institution of Electrical Engineers.

Menezes AJ, van Oorschot PC and Vanstone S(1996). *Handbook of Applied Cryptography*(780 pp.). Boca Raton, FL: CRC Press.

Mouly M and Pautet M-B(1992). *The GSM System for Mobile Communications*(701 pp.). M. Mouly and MB Pautet.

Niemi V and Nyberg K(2003). *UMTS Security*(273 pp.). Chichester, UK: John Wiley & Sons.

Ojanperä T and Prasad R(1998). *Wideband CDMA for Third Generation Mobile Communications*(439 pp.). Boston: Artech House.

Patil, B et al. (2003). *IP in Wireless Networks*(372 pp.), Upper Saddle River. NJ: Prentice Hall.

Poikselkä M, Mayer G, Khartabil H and Niemi A(2004). *IMS IP Multimedia Subsystems Concepts and Services*(440 pp.). Chichester, UK: John Wiley & Sons.

Rantalainen T, Spirito MA and Ruutu V(2000). Evolution of location services in GSM and UMTS networks. *Proceedings Of the Third International Symposium on Wireless Personal Multimedia Communications* (*WPMC 2000*), *November*, *Bangkok*(pp. 1027 – 1032).

Redl SH, Weber MK and Malcolm WH(1995). *An Introduction to GSM*(379 pp.). Boston: Artech House.

Spirito MA (2000). Mobile stations location estimation in current and future TDMA mobile communication systems. Ph. D. thesis. Politecnico di Torino. Facoltà di Ingegneria.

Stallings W (2000). *Data and Computer Communications* (810 pp.). Englewood Cliffs, NJ: Prentice Hall.

Viterbi AJ(1995). *CDMA Principles of Spread Spectrum Communications*(254 pp.). Reading, MA: Addison-Wesley.

版 权 声 明

Original edition, entitled *UMTS Networks: Architecture, Mobility and Services*, Second Edition by Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamäk Naghian, Valtteri Niemi, ISBN 0-470-01103-3, published by Wiley Publishing, Inc.



UMTS Networks
Architecture, Mobility and Services (Second Edition)

3G技术与UMTS网络（第2版）

“最好的UMTS著作，与其他同类图书相比，不仅全面而出色地阐述了理论，而且更重要的是，有丰富的实践知识。”

—— Amazon.com

UMTS是3G移动通信的主流核心技术，而且有望继续演进，在4G移动通信中发挥更大作用。

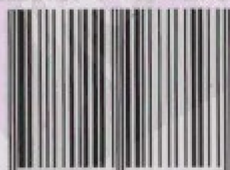
本书是全球移动通信巨头Nokia公司研究中心多位资深研究员多年经验的结晶，全面探讨了UMTS技术的来龙去脉和各方面细节，第1版出版后获得广泛赞誉，成为公认的名著。新版根据3GPP协议标准新版本的进展做了大幅修订，详细讲述了HSPDA、GSM/EDGE、IMS等关键技术。

全书图文并茂、实例丰富、条理清晰，既适合移动通信科研和管理人员阅读，也可以作为高校相关专业教材。



WILEY
www.wiley.com





ISBN 978-7-115-18772-7
9 787115 187727 >
ISBN 978-7-115-18772-7/TN
定价：59.00 元

本书相关信息请访问：图灵网站 http://www.turingbook.com
读者/作者热线：(010) 88593802
反馈/投稿/推荐信箱：contact@turingbook.com

分类建议 电子电气/移动通信

人民邮电出版社网址 www.ptpress.com.cn